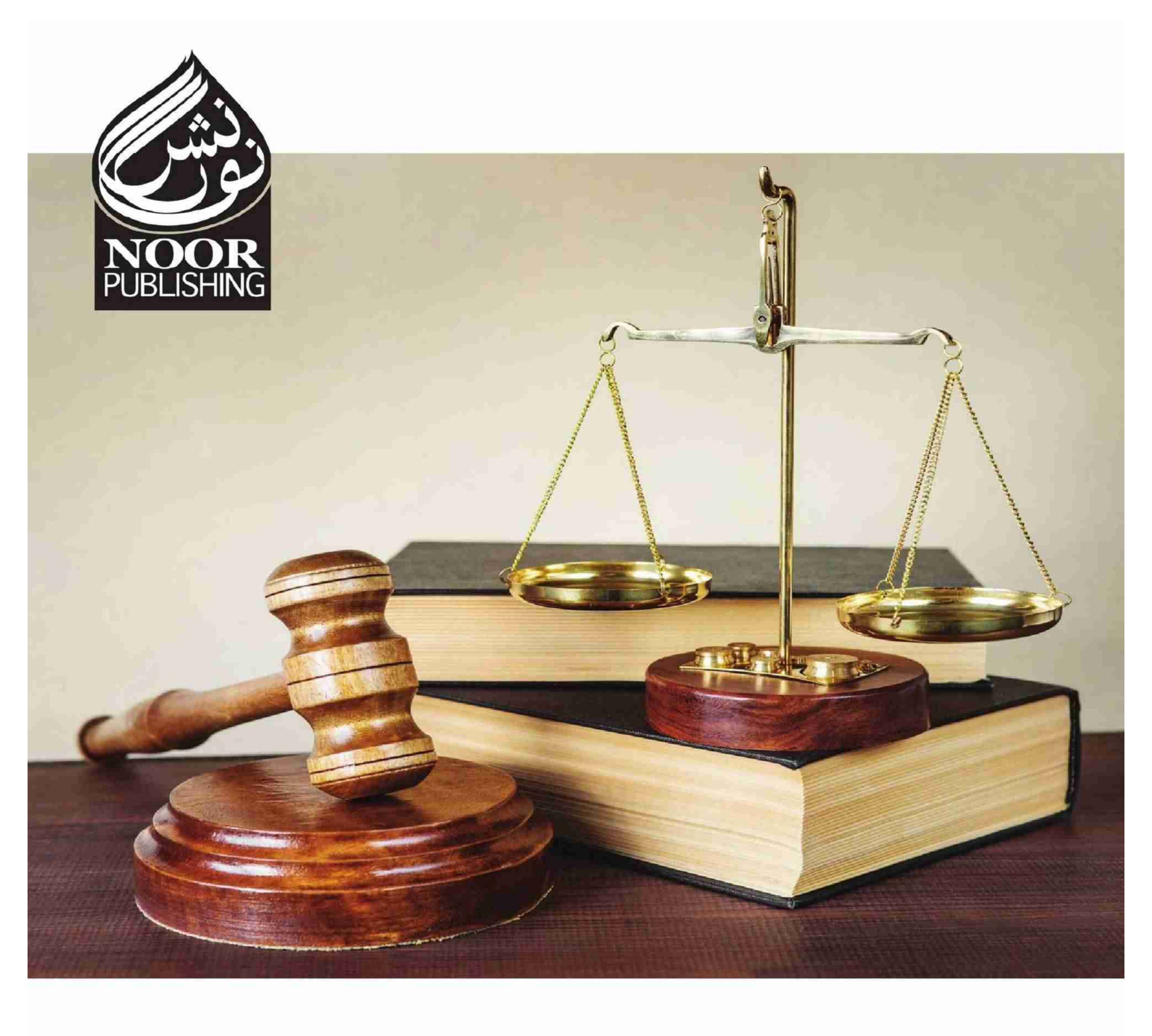


نادر الغزوانى

الحماية الجنائية من جرائم الإنترنت

دراسة مقارنة

الحماية الجنائية من
جرائـم الإنـترنت

دراسة مقارنة

نادر عبد الكريم الغزوانى

عَلَّمَ الْإِنسَانَ مَا لَمْ يَعْلَمْ

سورة العلق/ الآيه 5

الإهداء

الى روح والدى الطاهرة

المقدمـــة :

الحمد لله الذى نحمده ونستعينه ونستغفره ونتوب إليه من كل الذنوب ونعوذ بالله من شرور أنفسنا وسيئات أعمالنا ، من يهد الله فلا مضل له ومن يضلل فلا هادى له ونشهد أن لا إله إلا الله وحده لا شريك له ونشهد أن محمد عبده ورسوله.

أما بعد .....

لا شك أن التطور الذى يشهده العالم منذ فترة ليست بالقصيرة وإنتشار شبكة المعلومات الدولية (Internet) فتح مجالات عدة لإستفادة الكثيرين ، ولكن وبالرغم من ذلك فإن لهذا التطور مضار كثيرة لا سيما فى مجتمعنا الإسلامى والعربى حيث أفرزت هذه التقنيات نوعاً جديداً من الجرائم لم نألفها من قبل ألا وهى جرائم الإنترنت ، وهى جرائم تختلف كلياً عن باقى الجرائم مع ملاحظة أن الضرر الناجم عنها لا يمكن فصله عن الأضرار الناتجة عن الجرائم الأخرى.

وجرائم الإنترنت ترتبط لزوماً بوجود حاسب آلى متصل بشبكة المعلومات الدولية ولذلك قد تسمى هذه الجريمة أيضاً بإسم الجريمة المعلوماتية ، وبالعودة للحديث عن الشبكة الدولية للمعلومات (الإنترنت) فقد فاقت هذه الشبكة جميع وسائل الإعلام الأخرى من حيث السرعة فى تقديم المعلومات وتحصيلها ، وكذلك من حيث التنصل من الرقابة المفروضة من قبل السلطات فالدولة وإن كانت تستطيع فرض رقابتها بل ووصايتها أحياناً على صحافتها وإعلامها ووضع الخطوط الحمراء الممنوع تجاوزها، فإن الإنترنت له رأى آخر فى هذا الصدد حيث أن المعلومات تنتقل من خلال هذه الشبكة من مكان لآخر ومن دولة لأخرى أو لدول أخرى كثيرة فى لحظات دون حراس أو قيود أو (رقابة).

فالإنترنت ينقل لك المعلومات ويوصلها إليك فى عقر دارك دون أن تكلف نفسك عناء وإن كانت هذه ميزة فهى قد تحمل فى طياتها الخطر، فالجانب الآخر من الإنترنت يحوى عديد الأضرار مع الإشارة إلى أن إستخدامنا له هو الذى يحدد ما إذا كان مفيداً أو ضاراً.

وبشكل أكثر تبسيطاً فإن جرائم الإنترنت هى نتاج إستخدام سلبى لهذه التقنية ، فالجرم ليس فى التقنية بحد ذاتها ولكن الجرم والخلل فيمن يقوم بتوظيفها لهذا الغرض.

أهمية الموضوع :

تبرز أهمية دراسة هذا الموضوع فى ظل عدم وجود نصوص قانونية خاصة بجرائم الإنترنت ، وبإعتبار أن لا عقوبة إلا بنص فإن هذا الأمر يستوجب إعادة النظر بالتشريعات

القائمة لتعديل بعض نصوصها، إضافةً لضرورة صياغة نصوص عقابية خاصة بهذه الجريمة التى تعد نوعية جديدة على بساط القانون ولم يتناولها القانون الجنائى التقليدى ، فمثلاً يفتقر قانون العقوبات لنص يجرم القذف والسب عن طريق الإنترنت أو يجرم سرقة المعلومات المخزنة إليكترونياً.

وكذلك تتحدى جرائم الإنترنت الأجهزة الأمنية والقضائية بثغرات ليست بالهينة ، فيمكن مثلاً القيام بعملية إحتيال تتم بين دولتين (ألمانيا . أسبانيا) بينما المرتكب أو المنفذ لهذه العملية يوجد فى دوله ثالثة (إيطاليا مثلاً) وهذا الأمر يثير مشاكل قانونية فيما يتعلق بالإختصاص القضائى والإثبات ، ومازالت الأجهزة القضائية وأساتذة القانون فى العالم دون إستثناء عاجزين عن الخروج بتصور واضح عن الجريمة وتفرعاتها الكثيرة المختلفة وإن كانت الأنظمة القانونية المختلفة تحاول إيجاد وتأسيس أرضية قانونية واضحة حول هذه الجرائم.

صعوبة البحث:

تكمن صعوبة هذا البحث فى ضرورة الإلمام بكل ما يتعلق بشبكة الإنترنت ، وكيفية عملها ومعرفة المقصود بمواقع الإنترنت وفهم المصطلحات اللغوية والهندسية المحيطة بها وكيفية تصور إرتكاب جرائم من خلالها وقياس هذه الجرائم على الجرائم العادية لإمكانية التعامل معها قانوناً.

خطة البحث:

تأتى دراستنا للموضوع فى فصلين يسبقهما مبحث تمهيدى نتعرف فيه على ماهية شبكة الإنترنت وماهى خصائصها ومميزاتها ، وكذلك التعريف بماهية وكيفية إرتكاب جرائم الإنترنت وبيان خصائصها وسمات مرتكبيها.

أما الفصل الأول فسوف نخصصه لتفصيل وبيان بعضاً من جرائم الإنترنت وقسمنا الدراسة فيه إلى مبحثين سنتناول فى أحدهما الجرائم التقليدية التى ترتكب على الشبكة ، وفى المبحث الثانى سنتناول الجرائم المستحدثة التى أفرزها الإلمام العالى من قبل مرتكبيها بهذه التقنية.

أما الفصل الثانى فسنتناول فيه الجهود المبذولة لمكافحة جرائم الإنترنت سواء كانت هذه الجهود جهوداً وطنية على المستوى الداخلى لكل دولة ، أو جهوداً على المستوى الدولى تتطلب تكاتف أكثر من دولة للقضاء على مثل هذا النوع من الجرائم.

وسيكون مخطط الدراسة على النحو التالى:

المبحـــث التمهيـدى

المدلول العام لشبكة الإنترنت والجرائم المترتبة عليها

المطلب الأول : التعريف بشبكة الإنترنت وبيان خصائصها.

الفرع الأول : التعريف بشبكة الإنترنت.

الفرع الثانى : خصائص شبكة الإنترنت.

الفرع الثالث : إستخدامات شبكة الإنترنت.

المطلب الثانى : التعريف بجرائم الإنترنت وبيان خصائصها وسمات مرتكبيها.

الفرع الأول : تعريف جرائم الإنترنت.

الفرع الثانى : خصائص جرائم الإنترنت.

الفرع الثالث : مجرم الإنترنت.

الفصــل الأول

الجرائــم المرتكبــة بواسطـــة الإنـترنت

المبحث الأول : الجرائم التقليدية المرتكبة بواسطة الإنترنت.

المطلب الأول : جرائم القذف والسب.

المطلب الثانى : جريمة الإعتداء على حرمة الحياه الخاصة.

المطلب الثالث : الجرائم المخلة بالآداب العامة.

المبحث الثانى : الجرائم المستحدثة المرتكبة بواسطة الإنترنت.

المطلب الأول : الجرائم الواقعة على التجارة الإليكترونية.

المطلب الثانى : جرائم الإتلاف المعلوماتى.

المطلب الثالث : جرائم غسيل الأموال.

الفصل الثانى

مكافحـــة جرائـــم الإنـــترنت

المبحث الأول : مكافحة جرائم الإنترنت على المستوى الوطنى.

المطلب الأول : سبل الحماية الفنية فى مواجهة جرائم الإنترنت.

المطلب الثانى : التصدى الشرطى لجرائم الإنترنت.

المبحث الثانى : مكافحة جرائم الإنترنت على المستوى الدولى.

المطلب الأول : التعاون الشرطى والقضائى على المستوى الدولى.

المطلب الثانى : الإتفاقيات والمؤتمرات الدولية.

المطلب الثالث : معوقات التعاون الدولى.

المبحث التمهيدى

المدلول العام لشبكة الإنترنت والجرائم المترتبة عليها

تمهيـــد :

تعتبر شبكة الإنترنت أضخم شبكة كمبيوتر على مستوى العالم، تندمج فيها كلاً من تكنولوجيا الحاسب الآلى مع تكنولوجيا الإتصالات ، الأمر الذى جعلها من الأهمية بحيث لا يمكن الإستغناء عنها فى كثير من المجالات سواء كانت تجارية أو علمية بحثية أو خدمية أو مصرفية.

ولكن هذا التطور التكنولوجى الهائل لا يمكن أن ننظر اليه من جانب إيجابى فقط حيث أن إزدياد العمل به أدى إلى إفراز جانب سلبى لا يمكن إغفاله أو غض الطرف عنه.

ولذلك فإننا فى هذا المبحث سوف نقوم بتعريف شبكة الإنترنت وإبراز خصائصها وإستخداماتها فى مطلب أول.

ثم فى المطلب الثانى سوف نعرف جرائم الإنترنت ونبين خصائصها بالإضافة لبيان سمات مرتكبى هذا النوع من الجرائم.

المطلـــب الأول

التعريف بشبكة الإنترنت وبيان خصائصها وإستخداماتها

فى هذا المطلب سوف نقوم بتعريف شبكة الإنترنت بالإضافة إلى تبيان أهم خصائصها واستخداماتها وذلك على النحو التالى:

الفـــرع الأول

التعريـــف بشبكـــة الإنـــترنت

يمكن تعريف شبكة الإنترنت . وفقاً لما نعتقده صحيحاً . بأنها الشبكة الدولية العملاقة التى يندرج تحت لوائها عدد لا محدود من الشبكات وأجهزة الحاسب الآلى، بما تحويه من معلومات والمرتبطة ببعضها البعض بعدة وسائل قد تكون سلكية كالخطوط الهاتفية، أو لاسلكية كالأقمار الإصطناعية لذلك يطلق عليها أيضاً إسم (شبكة الشبكات) على إعتبار أنها الشبكة الأم التى تحوى باقى الشبكات.ومصطلح الإنترنت هو إختصار للمسمى الإنجليزى (International Communication Network):

وكذلك تعرف بأنها شبكة فضائية تنتقل من خلالها المعلومات بطريقة رقمية بين مجموعة من الحاسبات الآلية(1).

ومن تعريفاتها أيضاً أنها شبكة عالمية دولية ووسيلة من وسائل الإتصال والتواصل بين الشبكات تجمع بين مجموعة من أجهزة الحاسب الآلى المرتبطة ببعضها البعض، إما عن طريق خطوط التليفون، أو عن طريق الأقمار الصناعية وتعمل وفقا لبروتوكول وحيد (Tcp/ip) حيث تقدم للإنسانية جملة من الخدمات كالبريد الإليكترونى وتبادل المعلومات(2).

وكذلك يمكن أن تعرف شبكة الإنترنت بإعتبار جانب المعلوماتية فيها بأنها (دائرة معارف عملاقة يمكن للناس من خلالها الحصول على المعلومات حول أى موضوع فى شكل نص مكتوب أو رسوم أو صور أو خرائط أو التراسل عن طريق البريد الإليكترونى)(3).

ولشبكة الإنترنت عدة مسميات أو مرادفات فقد تسمى الشبكة العنكبوتية أو الشبكة العالمية أو شبكة الويب وكلها مسميات تصب فى نفس المعنى او المقصود.

---

(1) د.ماجد راغب الحلو، العقود الادارية، دار الجامعة الجديدة ،2007، ص107.

(2) نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الإستدلالات ، دراسة مقارنة ، دار الفكر الجامعى،2007 ، ص6-7.

(3) د. محمد خليفة العمرى، واقع إستخدام الإنترنت لدى أعضاء هيئة التدريس وطلبة جامعة العلوم والتكنولوجيا الأردنية، مجلة إتحاد الجامعات العربية، العدد 40 ، ربيع الثانى 1423هـ ، ص39.

وقد ظهر أول تصور نظرى مكتوب لفكرة إتصال الحاسبات عن طريق شبكة إتصال فى أغسطس من العام 1962 فى مذكرات كتبها (Licklider) الذى كان أول رئيس لمركز أبحاث الكمبيوتر (Darpa) وبالفعل تم إجراء أول إتصال بين حاسبين فى مدينتين مختلفتين عام 1965 عن طريق خط الهاتف وكان أحد الحاسبين من نوع TX_2 والآخر من نوع Q _ 32 [(1)].

وتعتبر الولايات المتحدة هى صاحبة السبق فى إنشاء شبكة الإنترنت، ففى عام 1969 تحديداً بدأت وزارة الدفاع الامريكية بإنشاء مشروع دفاعى يقوم على ربط الحواسيب الآلية الخاصة بوزارة الدفاع بالجهات المختصة بإجراء البحوث العسكرية، والتى تضم أيضاً عدد من الجامعات التى تقوم بأبحاث خاصة لصالح الجيش الأمريكى وسميت هذه الشبكة باسم الأربانت (ARPA NET) وكلمة(ARPA) هى إختصار للإسم

(Advanced Research Project Agency net)

أى إدارة مشروعات الأبحاث المتقدمة وقد بدأت هذه الشبكة تعمل على نطاق عدد محدود من الولايات ثم سرعان ما امتدت لتشمل كافة الولايات المتحدة الامريكية.

وكان الهدف من ذلك النظام هو وضع القوات الأميركية فى حالة تأهب قصوى داخل مراكز إدارة الصواريخ ، خاصة فى حالة نشوب حرب نووية أو أى إعتداء عسكرى عليها[(2)]، لاسيما مع وجود الخطر السوفيتى وما يمثله من تهديد نووى فى مواجهة الولايات المتحدة، وبعد إنهيار الإتحاد السوفيتى وما أعقبه من إنتهاء للحرب الباردة إنتفت الحاجة لهذه الشبكة على الأقل من الناحية العسكرية وتحولت لما هى عليه الآن من خدمة للأغراض المدنية.

ففى بداية حقبة السبعينات وبإنضمام وكالة الفضاء الامريكية (NASA) والمؤسسة القومية للعلوم (NSF) ومراكز البحث العلمى أخذت الشبكة الطابع المدنى، وأصبح التمويل الخاص بها يتم عن طريق جهات حكومية وبإنضمام أعداد هائلة من الشبكات الخاصة بالشركات والمؤسسات، أخذت الشبكة الطابع التجارى بعد أن كانت مقتصرة على الجوانب الأكاديمية والعسكرية فقط[(3)].

---

(1) An article entitled Abrief history of the internet - available at: http://www.walthowe.com/navnet/history.html

(2) د.عبد الفتاح بيومى حجازى، الجرائم المستحدثة فى نطاق التكنولوجيا الحديثة، الطبعة الأولى ، منشأة المعارف ، 2009 ،ص23-24.

(3) د.يحيى مصطفى حلمى وآخرون ، أساسيات الحاسبات الاليكترونية، مكتبة عين شمس ، القاهرة، 1995،ص5.

وبالتالى إنقسمت الأربانت الى جزئين أو شبكتين ، إحداهما وهى الأساس الذى أنشئت من أجله الشبكة وإحتفظت بالإسم الأصلى الأربانت وهى الخاصة بخدمة الشق العسكرى ، أما الثانية فهى الخاصة بالإستخدامات العادية والسلمية لهذه الشبكة .

وفى فترة الثمانينات إنضمت عدة شبكات أخرى من عدد من الدول كفرنسا واليابان والمملكة المتحدة، وفى بداية التسعينات أصبحت شبكة الإنترنت تغطى معظم دول العالم تقريبا وإنضمت إليها آلاف الشبكات فعام 1990 شهد دخول شبكة ويب (Web) التى تتميز بإمكانية إستخدام تقنية الصوت والصورة وأدوات الإعلام المتعددة [1].

أما عن وقت دخول شبكة الإنترنت إلى البلدان العربية فقد دخلت في أواخر الثمانينات بشكل محدود جداً، ولم يتوسع إستعمال شبكة الإنترنت في البلاد العربية إلا منذ أوائل التسعينات من القرن الماضي.

الفرع الثانــى
خصائــص شبكـــة الإنـترنت

تتميز شبكة الإنترنت بعدد من الخصائص والمميزات نجملها فى الاتى:

1- سهولـــة الإستخدام:

يتميز الإنترنت بسهولة إستخدامه حيث يكفى أن يكون الشخص ملماً بأساسيات الحاسب الآلى وكيفية إستخدامه وتشغيله ، ثم بعد ذلك الدخول للبرنامج المعد للتصفح عبر شبكة الإنترنت عن طريق النقرعلى الأيقونة الخاصة بشبكة الإنترنت والموجودة على شاشة الكمبيوتر، مع القليل من الإرشادات والتوجيهات ممن لهم سابقة التعامل فى هذا المجال يستطيع الشخص بعدها تصفح ما يشاء من مواقع الإنترنت وذلك بكتابة اسم الموقع الذى يريد التصفح داخله.

2- قلة التكاليف:

يتاح للمستخدم الإتصال بشبكة الإنترنت مقابل مبلغ مالى معين يقوم بدفعه للشركة المسئولة عن تقديم الخدمة، وهو عبارة عن إشتراك شهرى يتحدد حسب إستهلاك المستخدم وهو مبلغ زهيد مقارنة بكم المعرفة المخزنة داخل تلك الشبكة.

إضافة لذلك تمثل الإنترنت أداة فعالة لإنجاز الكثير من المهام بكلفة منخفضة ، فكلفة

(1) محمد عبد الله أبو بكر سلامة ، موسوعة جرائم المعلوماتية (جرائم الكمبيوتر والإنترنت) منشأة المعارف ، 2006 ، ص34.

رسالة البريد الإليكترونى لا تذكر قياسا بكلفة البريد العادى ، وكلفة الكتاب الإليكترونى والبرنامج الإليكترونى عادة أقل كلفة من مثيله العادى، وكلفة هاتف الإنترنت فى المكالمات الدولية لا تقارن بكلفة الهاتف العادى(1).

3- الفوريـــة:

ألغت الإنترنت حاجزى الزمان والمكان ، فالإتصال يتم بشكل مباشر بغض النظر عن مكان الشخص المرسل أوالشخص المستقبل ، فليس هناك حاجة لإنتظار وصول الرسائل البريدية للإطلاع على أخبار الأهل أو الأصدقاء ،أو إنتظار صدور الجريدة للإطلاع على الأخبار المحلية أو العالمية فالإنترنت يقوم بذلك ، حيث أن هذه التقنية تعمل طوال 24 ساعة يومياً على مدار الأسبوع وطيلة أيام السنة(2).

4- التواصل المستمر:

خاصية أخرى يتفرد بها الإنترنت وهى التواصل بين مستخدميه ، فأنا كمستخدم له أستطيع التواصل مع شخص آخر فى دولة أخرى تقع فى قارة أخرى من قارات العالم فأرسل له بريد إليكترونى يستطيع أن يجيبنى عليه فى نفس الوقت دون إنتظار، ويستطيع أى مستخدم مثلا أن يحصل على فتوى دينية مثلا فى نفس الوقت من أحد المواقع المتخصصة فى ذلك هذا كله بخلاف ما قد يستطيع المتصفح الحصول عليه من معلومات مستجدة على مدار الساعة بعكس وسائل الاعلام الاخرى.

5-الإنتشار والتطور:

شبكة الإنترنت وجدت ليس لتقف عند حد معين، ولكنها شبكة متطورة دائمة التغير والتجديد ، فكل يوم يشهد إنضمام العديد من المستخدمين لهذه الشبكة وكذلك تزايد عدد المواقع الإليكترونية والتحديث المستمر للمواقع الموجودة فعلا ،حيث أن المستخدم لا يكاد يكمل التصفح فى موقع إلا ووجد نفسه قد ولج الاخر.

6- العالمية:

لا تعترف الإنترنت بالحواجز المكانية أو الجغرافية فالعالم بين يديك وداخل شاشتك الصغيرة وبضغطة زر واحدة دون أى مشكل تستطيع التجول بين دول العالم ومشاهدة أبرز معالمها، و كذلك تستطيع التسوق من خلال الإنترنت ومشاهدة ما تشاء من السلع وأنت فى

---

(1) أنظر د .على بن عبد الله عسيرى ،الآثار الأمنية لإستخدام الشباب للإنترنت ، جامعة نايف العربية للعلوم الأمنية، الرياض ، الطبعة الأولى ،1425هـ ،ص26.

(2) د .على بن عبد الله عسيرى ، المرجع السابق ، ص 23.

منزلك[1].

7- عدم إمكانية التحكم بها:

بخلاف وسائل الإعلام الأخرى التى لها إدارة ومرجعية يمكن الرجوع اليها وإلزامها بضوابط وقوانين معينة ، ليس للإنترنت مرجعية معينة يمكن فرض القوانين عليها والمواد التى توضع على الإنترنت تصدر عن مصادر لاحصر لها لذلك شكلت الإنترنت تحديا أمنياً وقوياً يصعب التعامل معه[2].

الفــرع الثالــث

إستخدامـــات شبكـــة الإنترنت

1. الإستخدامات الإتصالية:

تعتبر الإنترنت فى الأساس وكما ذكرنا فى تعريفنا لها وأسباب نشأتها وسيلة إتصال، ولعل هذا هو السبب الرئيسى فى وجوده حيث حلت الإنترنت محل وسائل الإتصال العادية فالبريد الإليكترونى أصبح بديلا للبريد العادى ، والمكالمات الهاتفية عبر الإنترنت والتى تعتبر أقل كلفة حلت محل الإتصالات التليفونية وهو مازاد من إعتماد الناس عليه كوسيلة إتصال أوفر وأسرع.

2. الإستخدامات التعليمية:

يستخدم الإنترنت فى مجال التعليم فى عدة نواحى كما يلى:

أ– التعليم عن بعد:

تحقق الإنترنت إمكانية إيجاد فصول بلا جدران مما يمكن الطلاب من متابعة دروسهم على بعد آلاف الأميال من جامعاتهم ، وهذا من شانه أن يعالج مشكلة تكدس الطلاب فى الجامعات وقد بدأ بالفعل تطبيق هذا المفهوم فى التعليم ومن أمثلة ذلك : معهد ماساتشوستش للتكنولوجيا (MIT) الذى يقدم برنامجا للماجستير فى إدارة الأنظمة دون الحاجة لحضور الطلاب الى المعهد ، كما تقدم أكاديمية جورجيا الطبية 200 فصل دراسى مرتبطة بها فى

---

(1) راجع فى ذلك ، د. على بن عبد الله عسيرى ، المرجع السابق ، ص23.

(2) د.عبد الرحمن عبد العزيز السبيعى ، حرب المعلومات ، مرامر للطباعة الاليكترونية ، بدون تاريخ، ص285.

مختلف انحاء العالم يستطيع الطلاب من خلالها دراسة عدد من المواد والإختبار فيها[1].

كذلك توجد عدة جامعات عربية على الإنترنت من بينها جامعة العرب الاليكترونية (www.arabuniversty.com)

ب- التعليم المستمر:

تتزايد الحاجة إلى التعليم المستمر مع تسارع التطورات فى عصرنا الحاضر مما يتحتم تدريب العاملين لمواجهة التطورات والمستجدات وتدريب الموظفين ، و يوجد كثيرا من التعقيدات لصعوبة الاستغناء عن جهود العاملين فى جهات عملهم لذلك فإن التعليم عن طريق الإنترنت يشكل بديلا مناسبا وفاعلاً فى هذه الفرضية إذ يستطيع العاملون فى مختلف القطاعات حضور الدورات التدريبية دون أن يضطروا لمغادرة أماكن عملهم[2].

3. الإستخدامات العلمية[3] :

يزخر الإنترنت بملايين المواقع التى تحتوى على كم هائل من المعلومات فى شتى مجالات المعرفة وعلى عدة أشكال منها:

أ – المكتبات الإليكترونية:

توجد مكتبات إليكترونية على الإنترنت تحوى كتبا كاملة فى شتى التخصصات كمكتبات المواقع الطبية والتجارية والحكومية، وكذلك المكتبات الإسلامية بحيث تستطيع من مكانك الإطلاع على أحدث إصدارات الكتب بل وتحميلها على حاسبك الآلى .

والجدير بالذكر أن تلك الخدمة قد تكون مجانية وقد تكون بمقابل كما هو الحال فى أغلب المواقع.

ب- قواعد البيانات:

وهى عبارة عن معلومات مجمعة ومصنفة بطريقة معينة بحيث تقدم للباحثين أكبر قدر من الإستفادة مثال ذلك دوائرة المعارف العامة والمتخصصة، ويستفيد الباحثون من قواعد البيانات لأنها تشكل دائرة معارف عملاقة وتتيح المعلومات اللازمة لكافة الباحثين.

---

(1) د.عبد الله بن عبد العزيز الموسى ، إستخدام خدمات الإنترنت بفاعلية فى التعليم، مقال منشور بالانترنت، راجع الموقع ، www.riyadhedu.gov.sa/alan/fntok/12.htm

(2) د. على بن عبد الله عسيرى ، المرجع السابق ، ص35.

(3) أنظر فى ذلك د.على بن عبد الله عسيرى ، المرجع السابق ، ص 31 . 34.

ج- البحث المباشر عن المعلومة:

يستطيع الباحث عن طريق محركات البحث والفهارس الموضوعية الموجودة داخل شبكة الإنترنت البحث عن أى معلومة تهمه .

د- النشر:

لأن الإنترنت وسيلة من وسائل العلم والتعليم، فقد إتجه العديد من الكتاب إلى نشر كتبهم على شبكة الإنترنت الأمر الذى يضمن نسبة إطلاع أكبر على الكتب وكذلك زيادة نسبة الربح.

4. الإستخدامات الحكومية:

يمكن للجهات الحكومية أن تتواصل مع جمهورها من خلال الإنترنت بحيث توصل إليهم الأنظمة والتعليمات وتتلقى منهم المقترحات والشكاوى والمراجعات، مما يوفر على المراجعين عناء الإنتقال والإنتظار ويوفر على الجهات الحكومية الجهد والنفقات(1).

5. الإستخدامات الأمنية:

فى وقتنا هذا لا تكاد تخلو أى وزارة للداخلية فى أى دولة من وجود موقع إليكترونى لها على شبكة الإنترنت لتتواصل مع الجمهور، الأمر الذى يوفر الكثير من الوقت فى حالات البلاغات والإنذارات عن الكوارث ونشر صور المطلوبين وكذلك الإسهام فى تحسين العلاقة المتوترة نوعاً ما بين المواطن وأجهزة الشرطة لاسيما فى بلداننا العربية وكذلك الإستفادة من الإنترنت فى نشر حملات التوعية المختلفة.

6. الإستخدامات الطبية:

للإنترنت أيضاً إستخدامات عديدة فى المجال الطبى، فعلى سبيل المثال توجد آلاف المواقع الطبية المنتشرة على الشبكة والتى يستطيع أى شخص أن يطلع عليها للحصول على كافة المعلومات الخاصة بالوقاية من أى مرض .

ليس هذا فقط بل يستطيع أيضاً الأطباء الإستفادة من الإنترنت فى عقد المؤتمرات الطبية عن بعد دون الحاجة للسفر، وكذلك يتاح للأطباء تجديد معلوماتهم وإضافة الكثير الى خبراتهم من خلال المعلومات الطبية المتاحة على شبكة الإنترنت.

7. الإستخدامات التجارية:

يستفاد من الإنترنت فى المجال التجارى على النحو التالى:

---

(1) د.على عبد الله عسيرى، مرجع سابق،ص37.

أ – التسوق عبر الإنترنت:

يمكن التسوق عبر الإنترنت وذلك عن طريق مواقع إليكترونية خاصة بعرض بعض السلع كالملابس والبضائع والسيارات وفى هذه الحالة يمكن الشراء عن طريق بطاقات الإئتمان .

وإن كان التسوق عبر الإنترنت خدمة إيجابية يقدمها الإنترنت فهى خدمة محفوفة بالمخاطر كما سنرى بعد ذلك.

ب– الدعاية والاعلان:

الإنترنت وسيلة سهلة وميسرة للإعلان من خلالها عن أى سلعة .

جـ– سوق الأوراق المالية:

يمكن شراء وبيع الأسهم والأوراق المالية ومعرفة أسعار نزول وصعود المؤشرات عن طريق المواقع الإليكترونية التابعة للبورصات العالمية.

8. الإستخدامات الإخبارية:

إستخدام اخر هام للإنترنت وهو إعتماد وكالات الأنباء العالمية على شبكة الإنترنت لنقل الخبر عن طريق إنشاء مواقع اليكترونية خاصة بها على الشبكة، مثال ذلك موقع قناة العربية ، وغيرها من القنوات والشبكات الإخبارية.

بالإضافة للإستخدامات سالفة الذكر توجد كذلك عدة خدمات أخرى تقدمها الإنترنت يمكن تلخيصها فى الآتى[1]:

- **خدمة البريد الإلكتروني** : لإرسال واستقبال الرسائل ونقل الملفات مع أي شخص له عنوان بريدي بصورة سريعة جدا لا تتعدى دقائق وهى كذلك خدمة تتيح للمستخدم إرسال وإستقبال الرسائل سواءً كانت فى شكل نصوص أو صور ثابتة ومتحركة أو رسائل صوتية.
- **قوائم العناوين البريدية** : تشمل إنشاء وتحديث قوائم العناوين البريدية لمجموعات من الأشخاص لهم اهتمامات مشتركة .
- **خدمة المحادثات الشخصية** : يمكن التحدث مع طرف آخر صوتا وصورة وكتابة.
- **خدمة الدردشة الجماعية** : تشبه الخدمة السابقة إلا انه يمكن التحدث مع أكثر من شخص في نفس الوقت حيث يمكن تنظيم مؤتمر لعدد من الأفراد.

---

(1) د. محمد عبد الله المنشاوى بحث بعنوان جرائم الانترنت من منظور شرعى وقانونى ، متوفر بالموقع الإليكترونى ، http://www.minshawi.com/old/internetcrim-in%20the%20law.htm

- **خدمة الاستعلام الشخصي :** يمكن الإستعلام عن العنوان البريدي لأي شخص أو هيئة تستخدم الإنترنت والمسجلين لديها.
- **خدمة تحويل أو نقل الملفات :** لنقل الملفات من حاسب إلى آخر.

المطلـــب الثانـــى

التعريف بجرائم الإنترنت وبيان خصائصها وسمات مرتكبيها.

فى هذا المطلب سوف نقوم بتعريف جريمة الإنترنت ونبين خصائصها وكذلك خصائص وسمات مرتكبى هذه الجرائم وذلك كما يلى :

الفــرع الأول

تعريــف جرائــم الإنــترنت

لا يوجد تعريف موحد ومتفق عليه من قبل الفقهاء والمهتمين بمثل هذا النوع من الجرائم حتى فى شأن تسميتها.

فهناك من يطلق عليها إسم- جرائم الحاسب الآلى والإنترنت- وهناك من يطلق عليها إسم -الجرائم الاليكترونية- وهناك من يطلق عليها اسم -الجريمة المعلوماتية - وهناك كذلك من يطلق عليها إسم -جرائم إساءة استخدام تكنولوجيا المعلومات والإتصالات- وهو ذات المسمى الذى ورد فى مشروع القانون العربى النموذجى الموحد فى شأن مكافحة هذه الجرائم(1).

وبالعودة للحديث عن تعريف جرائم الإنترنت فان هناك عدة تعريفات تناولت هذه الظاهرة وهى فى حقيقة الأمر تعريفات متفاوتة فيما بينها ضيقا وإتساعا حيث انه من الصعوبة وضع تعريف جامع مانع لها إذ أنها كما قيل تقاوم التعريف ولايوجد لها تعريف متفق عليه للدلالة عليها(2).

ويمكن تصنيف التعريفات التى تناولت جرائم الإنترنت الى عدة تصنيفات كالآتى:

1 ـ التعريفات التي تستند إلى موضوع الجريمة:

يمكن تعريف جرائم الإنترنت إستنادا إلى موضوع الجريمة، بأنها" كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات(3)، أوهى"الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة إستخدام المخرجات إضافةً إلى أفعال أخرى

---

(1) د.عبد الفتاح بيومى حجازى ، نحو صياغة نظرية عامة فى علم الجريمة والمجرم المعلوماتى، بدون دار نشر، الطبعة الأولى، 2009، ص32.

(2) محمد عبيد الكعبى ، الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت ، دراسة مقارنة ، دار النهضة العربية ، بدون تاريخ ، ص33.

(3) د. هدى قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن، الطبعة الأولى ، دار النهضة العربية، 1992 ، ص20

تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر [1].

وقد عرف جريمة الكمبيوتر خبراء متخصصون من بلجيكا في معرض ردهم على إستبيان منظمة التعاون الاقتصادي والتنمية (OCDE) ،حول الغش المعلوماتى عام 1982 تعريف مقتضاه ،أنها كل فعل أو إمتناع من شأنه الإعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[2].

2 ـ التعريفات التى تستند إلى وسيلة إرتكاب الجريمة:

بالنسبة للتعريفات التي إنطلقت من وسيلة إرتكاب الجريمة ، فإن أصحابها ينطلقون من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر وسيلة لإرتكاب الجريمة.

وبناءً على ذلك عرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها، "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيساً[3].

وكذلك عرفتها الشرطة البريطانية بأنها"إستعمال شبكة الحاسوب لعمل إجرامى"[4].

3 ـ التعريفات التى تستند على توافر المعرفة بتقنية المعلومات:

من هذه التعريفات تعريف وزارة العدل فى الولايات المتحدة الأمريكية، التى عرفتها بأنها" أى جريمة لفاعلها معرفة فنيه بتقنية الحاسبات يمكنه من إرتكابها[5].

ومن هذه التعريفات أيضاً تعريفها بأنها " أي فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر أساسية لإرتكابه والتحقيق فيه وملاحقته قضائيا[6].

وبنظرة تقييمية سريعة لما سبق، نجد أن كل إتجاه حاول تعريف جريمة الإنترنت من منظور معين أو زاوية واحدة ، وهذا تاكيداً لما بيناه فى البداية من صعوبة إيجاد تعريف شامل وجامع يعرف تلك الظاهرة .

---

(1) تعريف مذكور بالموقع : www.goa.gov.

(2) أنظر موقع المنظمة على الإنترنت : www.oecd.org.

(3) المحامى يونس عرب ، بحث بعنوان ، جرائم الكمبيوتر والإنترنت المعنى والخصائص والصور وإستراتيجية المواجهة القانونية، ص 7 ، البحث منشور على الإنترنت، راجع الموقع http://doc.abhatoo.net.ma/spip.php?article1200

(4) تعريف مذكور بموقع وزارة العدل بسلطنة عمان على الإنترنت : http://www.moj.gov.om/

(5) مشار له لدى ، محمد عبيد الكعبى ، مرجع سابق،ص34.

(6) المحامى يونس عرب، بحث بعنوان، جرائم الكمبيوتر والإنترنت المعنى والخصائص والصور وإستراتيجية المواجهة القانونية، المرجع السابق ، ص8.

وبالتالى لا يمكن الإعتماد فى تعريف تلك الجريمة على إتجاه واحد، بل يجب المزج بينها جميعا للوصول – حسب ما نظنه صحيحا– لمدلول واف لجريمة الإنترنت.

ولبيان ذلك فلعله من الصحيح القول بأن جرائم الإنترنت ، هى كل فعل غير مشروع بغض النظر عما إذا كان مجرم أو غير مجرم حسب قانون العقوبات (موضوع الجريمة)، يرتكب بإستخدام جهاز الحاسب الآلى (وسيلة الجريمة)، من قبل شخص له دراية وخبرة كبيرة بتقنية الحواسب الآلية (تقنية المعلومات).

الفــرع الثانـــى
خصائـــص جرائم الإنترنت

تتميز جرائم الإنترنت بعدة خصائص ومميزات تختلف عن باقى الجرائم التقليدية ومن أهمها ما يلى:

أولاً : الحاسب الآلى هو أداة إرتكاب الجريمة:

جريمة الإنترنت لابد وأن ترتكب عن طريق الحاسب الآلى، وهو أول أمر يميزها عن الجريمة التقليدية إضافةً إلى أن مرتكبها هو شخص يتمتع بخبرة فائقة فى مجال الحاسب الآلى والمعلوماتية.

ثانياً : جريمة دائمة التطور:

برغم حداثة جرائم الإنترنت، إلا إنها وبعكس باقى الجرائم الأخرى فى تطور مستمر ذلك أن أساليب إرتكاب هذه الجرائم من السهولة بحيث تنتقل من مكان لآخر فى ذات الوقت، فالمجرم الإليكترونى يستطيع التعرف على أجدى الطرق لإرتكاب الجريمة عن طريق الإتصال بأقرانه من مختلف دول العالم ،حيث أن جرائم الإنترنت تتميز بإمكانية تكوين تشكيلات إجرامية تضم العديد من الأفراد على المستوى الدولى، ويكون الربط بينهم عن طريق شبكة الإنترنت.

ثالثاً : جريمة عابرة للحدود:

فإرتكاب الجريمة قد يتم بالدخول إلى نظام حاسوب فى دولة ما عن طريق شخص يعيش فى دولة أخرى، الأمر الذى يثير تساؤلات عدة حول وقت إرتكاب الجريمة نظراً لإختلاف المواقيت الدولية عن بعضها البعض، وكذلك عن القانون واجب التطبيق على هذه الجريمة، هل هو قانون دولة إرتكاب الفعل الضار أم الدولة الحادث فيها الضرر.

رابعاً: عدم الإبلاغ عنها:

لا يتم – في الغالب الأعم – الإبلاغ عن جرائم الإنترنت إما لعدم إكتشاف الضحية لها

وإما خشيته من التشهير، لذا نجد أن معظم جرائم الإنترنت تم إكتشافها بالمصادفة، بل وبعد وقت طويل من إرتكابها، زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها . فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة ، والعدد الذي تم إكتشافه ، هو رقم خطير.

خامساً: سهولة إخفاء معالمها:

من السهل إخفاء معالم جريمة الإنترنت وصعوبة تتبع مرتكبيها، لذا فهذه الجرائم لا تترك أى أثرلها بعد إرتكابها ، علاوة على صعوبة الإحتفاظ الفني بآثارها إن وجدت ، فهذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ولذا فإن معظم جرائم الإنترنت تم إكتشافها بالمصادفة وبعد وقت طويل من إرتكابها.

سادساً: صعوبة كشف وملاحقة مرتكبها:

سبب ذلك أن الجانى غالبا ما يتلف أى أثر من الممكن أن يخلفه وراءه ، أضف لذلك أن إرتكاب الجريمة من خارج حدود الدولة وبوسائل تقنية متطورة قد يضيع الفرصة فى إكتشاف مرتكبها.

سابعاً: جريمة صعبة الإثبات :

تتميز هذه الجريمة بصعوبة إثباتها، ومرجع ذلك هو قلة عدد المتخصصين فى تعقب مثل هذا النوع من الجرائم حيث تنعدم الآثار التقليدية للجرائم كالبصمات مثلا، إضافة لسهولة محو وتدمير الدليل المادى فى زمن قصير جدا.

ثامناً:جريمة هادئة لا عنف فيها:

لا تحتاج جرائم الإنترنت إلى عنف أو مجهود كبير كما هو الحال فى الجرائم الإعتيادية التقليدية، وإنما تنفذ دون جهد يذكر ذلك أنها تعتمد على الخبرة المعلوماتية لدى مرتكبها.

تاسعاً: نقص الخبرة الفنية لدى الجهات المختصة بالتحقيق:

إكتشاف جرائم الإنترنت يتطلب إلماماً بالأمور الفنية والتقنية لدى أجهزة الشرطة والنيابة العامة والقضاء، وذلك للتوصل إلى مرتكبى مثل هذا النوع من الجرائم ذات التقنية المتطورة والأساليب المعقدة، الأمر الذى وجدت معه هذه الجهات نفسها أنها غير قادرة على التعامل مع هذا النوع من الجرائم[1].

---

(1) محمد عبيد الكعبى ، مرجع سابق ، ص39.

عاشراً: الفراغ التشريعى:

عند محاولة تطبيق القوانين التقليدية على جرائم الإنترنت، فلابد وأن نلحظ صعوبة إمكانية تطبيق تلك القوانين وذلك لخلوها من نصوص تشير لتلك الجرائم أو تحويها، فجريمة الإنترنت تستهدف رموزاً إليكترونية، وهو ما يفتقده قانون العقوبات مما يقلل من فرص إمكانية تطبيقه.

ومما زاد الطين بلة أنه لو فرضنا وجود قوانين متكاملة للوقاية من أخطار الإنترنت فى بلد من البلدان، فإن المعتدى يستطيع الإنطلاق من بلد لا توجد فيه قوانين صارمة لشن إعتداءاته فى بلدان أخرى توجد فيها تلك القوانين الصارمة، فتعجز البلد التى وقع عليها الاعتداء عن تطبيق قوانينها، ومن الأمثله على ذلك (فيروس الحب) الذى انتشر أواخر العام 2000 وكلف آلاف الشركات حول العالم خسائر تجاوزت المليارات، وعندما تم تحديد هوية الفاعل وجد أنه طالب فى الفلبين، وأنه لا يوجد فى الفلبين قانون يمكن محاكمته على أساسه[1].

(2) Dr. Phil Williams, An article entitled, Organized crime And crimes of the Internet, available at: http://usinfo.state.gov/journals/itgic/0801/ijga/comntry3.htm.

الفـرع الثالـث
مجـــــرم الإنــــترنت

يتميز مجرم الإنترنت عن المجرم التقليدى من عدة نواحى يمكن تلخيصها فى الآتى:

أولا : سمات مجرم الإنترنت:

1 – مجرم متخصص:

له قدرة فائقة في المهارة التقنية، ويستغل مداركه ومهاراته في اختراق الشبكات وكسر كلمات المرور أو الشفرات، ويسبح في عالم الشبكات ليحصل علي كل غالي وثمين من البيانات والمعلومات الموجودة علي أجهزة الحواسب ومن خلال الشبكات[1].

2– مجرم عائد للإجرام:

يتميز المجرم المعلوماتي بأنه عائد للجريمة دائما، فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات. فهو قد لا يحقق جريمة الاختراق بهدف الإيذاء وإنما نتيجة شعوره بقدرته ومهارته في الاختراق[2].

3– مجرم محترف:

له من القدرات والمهارات التقنية ما يؤهله لأن يوظف مهاراته في الاختراق والسرقة والنصب والاعتداء علي حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال[3].

4– مجرم ذكى:

حيث يمتلك هذا المجرم من المهارات ما يؤهله أن يقوم بتعديل وتطوير في الأنظمة الأمنية، حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب[4].

---

(1) د. فـؤاد جمـال ، جـرائم الحاسـبات و الإنترنـت ، بحـث منشـور علـى الإنترنـت راجـع الموقـع: http://www.tashreaat.com/view_studies2.asp?id=592&std_id=90

(2) د. فؤاد جمال، المرجع السابق.

(3) د. فؤاد جمال، المرجع السابق.

(4) د. فؤاد جمال ، المرجع السابق.

5- مجرم غير عنيف:

ينتمى الإجرام المعلوماتى إلى إجرام الحيلة فلا يلجأ المجرم المعلوماتى إلى العنف فى إرتكاب جرائمه فهذا النوع من الجرائم لا يستلزم مقداراً من العنف للقيام به(1).

6- مجرم إجتماعى الشخصية:

مجرم الإنترنت مجرم متكيف إجتماعيا، بحيث لا يضع نفسه فى حالة عداء سافر مع المجتمع المحيط به، بل إنه إنسان متكيف معه ذلك أنه أصلا إنسان مرتفع الذكاء ويساعده ذلك على عملية التكيف، وما الذكاء فى رأى الكثيرين سوى القدرة على التكيف ولا يعنى ذلك التقليل من شان هذا المجرم بل إن خطورته الإجرامية قد تزيد إذا زاد تكيفه الإجتماعى مع توافر الشخصية الإجرامية لديه(2).

ثانيا : تصنيفات مجرمى الإنترنت :

فى واقع الأمر يصعب وضع معيار محدد وتصنيف دقيق لمجرمى الإنترنت ولسماتهم وما يميزهم عن غيرهم من الجناة ، وذلك مرجعه قلة الدراسات الخاصة بالظاهرة وكذلك الحجم الكبير من جرائمها غير المكتشفة، أو غير المبلغ عن وقوعها، وكذلك بسبب النقص التشريعى الذى يحد من توفير الحماية الجنائية فى مواجهتها.

والغالب أن مرتكبى هذه الجرائم من الأفراد ذوو المهارات الفنية والتقنية العالية، فالإنترنت جريمة الأذكياء وأحد مشاكل الإنترنت أن المستعمل يكون مجهولا وغالباً ما يستخدم أسماء مستعارة بدلا من إسمه الحقيقى، فعدم تحديد الشخصية يشجع ويغرى الشخص على إرتكاب جرائم ما كان يفكر فيها(3).

ويتجه الباحثون إلى الإقرار بأن أفضل تصنيف لمجرمي التقنية هو التصنيف القائم على أساس أغراض الإعتداء حيث تم تصنيف مجرمي المعلومات إلى أربعة طوائف: المخترقون، المحترفون والحاقدون و أخيراً صغار السن(4).

1- المخترقون:

يتحد في إطار هذه الطائفة نوعين من المخترقين أو المتطفلين:

---

(1) د. سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية ، دار النهضة العربية ، 2007، ص22.

(2) د. سليمان أحمد فضل، المرجع السابق،ص22.

(3) http://reda79.jeeran.com/laweg/archive/2008/5/571259.html

(4) http://www.djelfa.info/vb/showthread.php?t=204052

- الهاكرز : (hackers)

الهاكر (hacker) أو المتسلل هو شخص بارع في إستخدام الحاسب الآلي وبرامجه ولديه فضول في إستكشاف حسابات الآخرين وبطرق غير مشروعة فالهاكرز، وكما يدل على ذلك إسمهم، هم متطفلون يتحدون إجراءات أمن نظم الشبكات، لكن لا تتوفر لديهم في الغالب دوافع حاقدة أو تخريبية وإنما ينطلقون من دوافع التحدي وإثبات الذات(1).

وكلمة (الهاكرز) هي كلمة تحمل المعنى (متخصص في نظم المعلومات والبرمجيات) وهي عبارة عن إسم إختاره لأنفسهم مجوعة من المبرمجين الأكفاء المهرة القادرين على إبتكار البرامج و القادرين أيضاً على حل مشكلات البرامج في الحاسب الآلي في جميع أنظمته(2).

- الكراكرز : (Crackers)

الكراكر أو المقتحم هو شخص يقوم بالتسلل إلى نظم الحاسوب للإطلاع على المعلومات المخزنة فيها أو لإلحاق الضرر أو العبث بها أو سرقتها، وكلمة كراكر هي كلمة تحمل في الإنجليزية معنى الكسر أو العبث والتحطيم ، وبالنسبة لموضوعنا فإن (الكراكرز) كلمة تعني التخريب،

وتهدف إعتداءات هذه الفئة بالأساس إلى تحقيق الكسب المادي لهم، أو للجهات التي كلفتهم وسخرتهم لإرتكاب جرائم الحاسوب (3).

2- مجرمو الحاسوب المحترفون:

وهم أكثر خطورة من الصنف الأول وقد يحدثون أضراراً كبيرة وقد يؤلفون أندية لتبادل المعلومات فيما بينهم(4).

ويتم تصنيف أفراد هذه الطائفة إلى مجموعات متعددة إما تبعا لتخصصهم بنوع معين من الجرائم، أو تبعا للوسيلة المتبعة من قبلهم في إرتكاب الجرائم.

---

(1) http://arabhardware.net/forum/archive/index.php/t-42072.html.
(2) http://arabhardware.net/forum/archive/index.php/t-42072.html.
(3) http://arabhardware.net/forum/archive/index.php/t-42072.html
(4) د. سليمان أحمد فضل ،المرجع السابق ، ص231.

3- الحاقدون:

هذه الطائفة يغلب عليها الرغبة بالإنتقام والثأر كأثر لتصرف صاحب العمل معهم أو لتصرف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها، ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوضعهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشأة المستهدفة في نشاطهم[1].

4- صغار السن:

أو كما يسميهم البعض صغار نوابغ المعلوماتية، و يوصفون بالصغار المتحمسين للحاسوب دافعهم التحدي لكسر الرموز السرية لتركيبات الحاسوب، و من الأمثلة الشهيرة لجرائم المعلوماتية لهذه الطائفة العصابة الشهيرة التي أطلق عليها إسم عصابة (414) و التي نسب إليها إرتكاب ستون فعل تعد في الولايات المتحدة الأمريكية على ذاكرات الحواسيب ، و أيضا عندما نجح بعض أفراد هذه الطائفة من الفرنسيين في إيجاد مدخل إلى الملفات السرية لبرنامج ذري فرنسي[2].

ويمكن رد الإتجاهات التقديرية لطبيعة هذه الفئة، وسمات أفرادها، ومدى خطورتهم في نطاق ظاهرة جرائم الحاسوب إلى إتجاهين رئيسيين :

- **الأول** : إتجاه لا يرى إسباغ أية صفة جرمية على هذه الفئة، أوعلى الأفعال التي تقوم بها، ولا يرى وجوب تصنيفهم ضمن الطوائف الإجرامية لمجرمي الحواسيب، إستنادا إلى أن صغار السن لديهم ببساطة ميل للمغامرة والتحدي والرغبة في الإكتشاف، ونادراً ما تكون أهداف أفعالهم المحظورة غير شرعية، وإستنادا الى أنهم لا يدركون ولا يقدرون مطلقا النتائج المحتملة التي يمكن أن تؤدي اليها أفعالهم غير المشروعة بالنسبة لنشاط منشأة أو شركة تجارية[3].
- **الثانى** : إتجاه يرى أن مرتكبي جرائم الحاسوب من هذه الطائفة يصنفون ضمن مجرمي الحاسوب كغيرهم دون تمييز إستنادا إلى أن تحديد الحد الفاصل بين العبث في الحواسيب وبين الجريمة أمر عسير من جهة، ودونما أثر على وصف الفعل – قانونا – من جهة

---

(1) المحامى يونس عرب، بحث بعنوان ، جرائم الكمبيوتر والإنترنت المعنى والخصائص والصور وإستراتيجية المواجهة القانونية، المرجع السابق ، ص 61 .

(2) Tom forester, Essential proplems to Hi-Tech Society, First MIT Pres edition,Cambridge, Massachusetts , 1989, P. 405.

(3) الأستاذ (أولريش سيبر) – جرائم الحاسب الآلي والجرائم الأخرى المرتبطة بالتقنيات الحديثة لوسائل الإتصال، ترجمة الدكتور سامي الشوا، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، 25–28، أكتوبر 1993 ، ص8.

أخرى، وإستناداً الى أن خطورة أفعالهم التي تتميز بإنتهاك الأنظمة وإختراق الحواسيب وتجاوز إجراءات الأمن، والتي تعد بحق من أكثرجرائم الحاسوب تعقيداً من الوجهة التقنية، ويدعم صحة هذا الإتجاه التخوفات التي يثيرها أصحاب الاتجاه الأول ذاتهم، إذ يخشوون من الخطر الذي يواجه هذه الطائفة، والمتمثل بإحتمال الإنزلاق من مجرد هاو صغير لإقتراف الأفعال غير المشروعة، إلى محترف لأعمال السلب، هذا إلى جانب خطر آخر أعظم، يتمثل في إحتضان منظمات الإجرام ومجرمين غارقين في الإجرام لهؤلاء الشباب[1].

ثالثاً : دوافع إرتكاب جرائم الإنترنت:

1- الفضول:

يعتبر الفضول غريزة إنسانية حبى بها الله بنى البشر فالإنسان دائماً ما يسعى لمعرفة خبايا الأمور ، وبناءً على هذا فإن مجرم الإنترنت قد لا يقصد إرتكاب أى فعل غير مشروع فى بداية الأمر ،ولكن حب الإستطلاع والفضول المتزايد قد يجره إلى مثل هذه الأفعال.

2- إثبات الذات:

فى هذه الحالة يسعى مجرم الإنترنت إلى تأكيد ذاته، وذلك عن طريق إختراق مواقع حكومية أو تابعة للدولة، حيث أنه من المعروف صعوبة إختراق مثل هذا النوع من المواقع وبالتالى يسعى المجرم فى هذه الفرضية لجذب الإنتباه إليه وإرضاء ذاته .

والصورة الذهنية لمرتكبي جرائم الحاسوب والإنترنت غالبا هي صورة البطل والذكي، الذي يستحق الإعجاب لا صورة المجرم الذي يستوجب محاكمته، فمرتكبو هذه الجرائم يسعون إلى إظهار تفوقهم ومستوى إرتقاء براعتهم، لدرجة أنه إزاء ظهور أية تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة، فيحاولون إيجاد الوسيلة إلى تحطيمها، أو التفوق عليها[2].

3- الرغبة فى الثراء:

المعروف أن جل الجرائم التى ترتكب يكون الغاية من ورائها جمع المال ، وكذلك الحال فى جرائم الإنترنت فحاجة المرء للمال قد تدفعه لإرتكاب مثل هذا النوع من الجرائم.

4- الرغبة فى الإنتقام:

الإنتقام موجود داخل النفس البشرية، فكثير من الأفراد يفصلون تعسفيا أو بغير وجه حق

(1) المحامى يونس عرب ، بحث بعنوان ، جرائم الكمبيوتر والإنترنت المعنى والخصائص والصور وإستراتيجية المواجهة القانونية، المرجع السابق ، ص 63.

(2) المحامى يونس عرب، المشار إليه أعلاه ، ص67.

من شركة أو منظمة حكومية، والبعض منهم قد يملكون المعلومات الكافية بخفايا هذه الجهة، لذلك يرتكب الجاني الجريمة رغبة منه في الإنتقام ليجعل الشركة أو المؤسسة تتكبد الخسائر المالية الكبيرة من جراء ما يسببه لها من ضرر يحتاج إصلاحه إلى وقت.

مثال ذلك ما قام به أحد المبرمجين فى إحدى الشركات العربية حيث وضع برنامجاً فى حاسب الشركة أدى إلى تدمير جميع ملفات الشركة المخزنة فى الحاسب الآلى بمجرد محو إسمه من كشف رواتب الشركة بعد فصله[1].

5- التسلية:

كما ذكرنا سابقاً أن من تصنيفات مجرمى الإنترنت (المخترقون) (الهاكرز والكراكرز) وهى فئه شغلها الشاغل هو العبث والتسلية ليس إلا، ولا يستهدفون أهدافاً أو أشخاصاً بعينها ولكن ما يهمهم هو الدخول لأجهزة الآخرين والعبث بها دون سابق معرفة بشخصية المجنى عليه.

6- دوافع عسكرية وسياسية:

شبكة الإنترنت -كما أوضحنا فى البداية- نشأت وتطورت من أجل أهداف عسكرية بحته، وحتى وقتنا الراهن من الممكن إستخدام هذه الشبكة كسلاح عسكرى فعال.

كما أن الإنترنت أصبحت وسيلة للدعاية العسكرية أستعملت فى مختلف الصراعات الماضية ، كما فعل الصرب فى أزمة كوسوفو حيث بثوا دعاياتهم بواسطة البريد الإليكترونى وكما تفعل إسرائيل فى محاولة تحسين صورتها أمام العالم فى مواجهة الإنتفاضة[2].

رابعاً : أهداف مجرم الإنترنت:

1. **المعلومات:**

ويشمل ذلك سرقة أو تغيير أو حذف المعلومات ، ومعظم تلك الجرائم التى يكون الهدف منها هو المعلومات هى فى الأغلب الأعم من الحالات تكون جرائم إقتصادية للحصول على مزايا أو مكاسب مادية ، فالحرب الإقتصادية لا تقل فى ضراوتها وشدتها حالياً عن الحرب العسكرية، إلا أنها تتم عبر شبكة الإنترنت[3].

---

(1) حسن طاهر داوود، جرائم نظم المعلومات، جامعة نايف العربية للعلوم الأمنية، الطبعة لاولى ،الرياض، 2000، ص135.

(2) د.على بن عبد الله عسيرى ، المرجع السابق ، ص64.

(3) د.سليمان أحمد فضل ،المرجع السابق ص21.

2. أجهزة الكمبيوتر:

ويشمل ذلك تعطيلها أو تخريبها ويتم ذلك غالباً عن طريق برامج الفيروسات.

3. الأشخاص والجهات:

هدف فئة كبيرة من الجرائم على شبكة الإنترنت أشخاص أو جهات بشكل مباشر كالتهديد أو الابتزاز. علماً بأن الجرائم التي تكون أهدافها المباشرة هي المعلومات أو الأجهزة تهدف بشكل غير مباشر إلى الأشخاص المعنيين أو الجهات المعنية بتلك المعلومات أو الأجهزة[1].

---

(1) http://shkoon.coolfreepage.com/amn/pages/amn-jra.htm

الفصـــل الأول

الجرائم المرتكبة بواسطة الإنترنت

تمهيد وتقسيم:

بالرغم من حداثة جرائم الحاسب الآلي والإنترنت نسبياً، إلا إنها لاقت إهتماما من قبل بعض الباحثين، حيث أجريت العديد من الدراسات المختلفة لمحاولة فهم هذه الظاهرة ومن ثم التحكم فيها، ومنها دراسة أجرتها منظمة (Software Alliance Busieness) في الشرق الأوسط حيث أظهرت أن هناك تباين بين دول منطقة الشرق الأوسط في حجم خسائر جرائم الحاسب الآلي حيث تراوحت ما بين (30) مليون دولار أمريكي في المملكة العربية السعودية والإمارات العربية المتحدة و (1.4) مليون دولار أمريكي في لبنان[1].

وقد أطلق مصطلح جرائم الإنترنت أو(Internet Crimes) في مؤتمر جرائم الإنترنت المنعقد في أستراليا بالفترة من 16 – 1998/2/17م[2].

وجرائم الإنترنت كثيرة ومتنوعة ويصعب حصرها، ولكن يجب الأخذ فى الإعتبار أن ثمة جرائم للإنترنت تتميز بأنها لاترتكب إلا عن طريق الإنترنت فقط وعن طريق جهاز الكمبيوتر، كجرائم نشر الفيروسات على الشبكة وإختراق وإقتحام المواقع ، والبعض الآخر من جرائم الإنترنت له شبيه على أرض الواقع كجرائم القذف والسب مثلاً، فهذه الجرائم قد ترتكب فى حق الأشخاص عن طريق الإنترنت ، أوعن طريق آخر.

وعلى هذا الأساس فإن دراستنا لجرائم الإنترنت فى هذا الفصل ستكون فى مبحثين على النحو التالى :

المبحث الأول : الجرائم التقليدية المرتكبة بواسطة الإنترنت.

المبحث الثانى : الجرائم المستجدة المرتكبة بواسطة الإنترنت.

---

(1) ذياب البداينة ، جرائم الحاسب والإنترنت ، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية ، الرياض ،1420 هـ ، ص98.

(2) عبد الرحمن محمد بحر، معوقات التحقيق فى جرائم الإنترنت، دراسة مسحية على ضباط الشرطة فى دولة البحرين،رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض،1420هـ ، ص2.

المبحـث الأول

الجرائم التقليدية المرتكبة بواسطة الإنترنت

تمهيد وتقسيم:

نقصد هنا بالجرائم التقليدية ، الجرائم التى ترتكب بشكل إعتيادى على شبكة الإنترنت من قبل مستخدميها ، أوهى الجرائم الأكثر شيوعاً بين مطالعى الشبكة بإعتبارهم جناة أو مجنى عليهم. وإرتأينا أن يكون محور دراستنا فى هذا المبحث على النحو التالى:

المطلب الأول : جرائم القذف والسب.

المطلب الثانى : جرائم الإعتداء على حرمة الحياة الخاصة.

المطلب الثالث : الجرائم المخلة بالآداب العامة.

المطلـب الأول

جرائـــم القـــذف والســـب

تعتبر جرائم القذف والسب من الجرائم الماسة بالشرف وبالإعتبار، ويقصد بالشرف والإعتبار المكانه التى يحتلها الشخص فى الوسط الاجتماعى المحيط به، سواء كان هذا الوسط هو مجتمع القرية أو الحى أو مجتمع الزملاء فى المهنة[1].

وبالتالى فإن المكانة الإجتماعية للفرد فى مجتمعه جديرة بتدخل المشرع لحمايتها من أى مساس بها سواءً عن طريق القول أو الكتابة.

وسنتناول فيما يلى كلاً من جريمتى القذف والسب وكيفية إرتكاب كلاً منهما عبر شبكة الإنترنت على التوالى.

الفـرع الأول

جريمـــــة القـــذف

تعريف القذف:

يعرف القذف بأنه:إسناد علنى عمدى لواقعة محددة تستوجب عقاب أو إحتقار من أسندت إليه[2].

وقد عرف القانون رقم 52 لسنة 1974م فى ليبيا القذف بأنه " الرمى بالزنا أو نفى النسب بأية وسيلة كانت وفى حضور المقذوف أو غيبته وفى علانية أو بدونها".

وقد سمى الله تعالى القذف رمياً، حيث قال فى كتابه الكريم:﴿ وَالَّذِينَ يَرْمُونَ الْمُحْصَنَاتِ ثُمَّ لَمْ يَأْتُوا بِأَرْبَعَةِ شُهَدَاءَ فَاجْلِدُوهُمْ ثَمَانِينَ جَلْدَةً وَلا تَقْبَلُوا لَهُمْ شَهَادَةً أَبَدًا وَأُوْلَئِكَ هُمُ الْفَاسِقُونَ ﴾. (سورة النور الآية رقم 4).

يتضح من التعريفات سالفة الذكر ، أن أساس القذف هو إسناد واقعة أو فعل معين لشخص معين،

ويشترط كذلك فى الإسناد أن يكون علنياً، وأن يحط ويقلل ويحقر من شأن المجنى عليه ، أما إذا لم يصل الإسناد لإحداث هذا الأثر فليس ثمة قذف فى حق المجنى عليه حتى ولو إعتبره كذلك.

---

(1) محمد عبد اللطيف عبد العال: حول مفهوم الشرف والاعتبار فى جرائم القذف والسب، مجلة الأمن والقانون، العدد الثانى، يوليو 2003م، أكاديمية شرطة دبى بالإمارات العربية المتحدة ص 290.

(2) د.حسنين إبراهيم صالح عبيد ، جرائم الإعتداء على الأشخاص ، دار النهضة العربية، 1983، ص199.

ونخلص مما سلف أن القذف المعاقب عليه قانوناً لابد وأن تتكامل شروطه وأركانه والتى تتمثل فى:

1- الركن المادى: الذى يتحقق

أ- بإسناد واقعة معينة إلى المجنى عليه لو صحت لأوجبت عقابه أو تحقيره.

ب- موضوع ينصب عليه الإسناد.

جـ- علانية الإسناد.

2- القصد الجنائى.(الركن المعنوى)

ونتناول كل ركن من هذه الأركان بشىء من التفصيل:

أولاً : الركن المادى لجريمة القذف:

1- فعل الإسناد:

يقصد بالإسناد نسبة أمر أو واقعة ما إلى شخص معين بأية وسيلة من وسائل التعبير عن المعنى، كالقول أو الكتابة أو الفعل وما يلحق بها، فكافة الوسائل التى تصلح للتعبير عن المعانى وتصويرها على نحو يمكن الغير من فهمها وإدراكها يصح أن يتحقق بها عنصر السلوك فى جريمة القذف[1].

أما بالنسبة للأسلوب الذى يتحقق به الإسناد فإن القاعدة أنه لا عبرة بالأسلوب الذى صاغ به الجانى عباراته ،أكان صريحاً بحيث لا يحتاج السامع أو القارىء إلى مجهود ذهنى لإستخلاص المعنى المقصود به، أم كان ضمنياً بحيث يتطلب فهمه مجهوداً يتكشف به المعنى الحقيقى الذى يستتر خلف معناه الظاهر وسواء الأسلوب الذى أفرغ فيه الإسناد الضمنى[2].

2-موضوع الإسناد:

ينبغى أن يكون موضوع الإسناد واقعة محددة، وأن يكون من شأن هذه الواقعة إن صحت عقاب من أسندت إليه أو إحتقاره عند أهل وطنه[3].

وإستلزام أن يكون موضوع الإسناد واقعة محددة هو العنصر الذى يتميز به القذف عن

---

(1) د. عمر السعيد رمضان ، شرح قانون العقوبات القسم الخاص، دار النهضة العربية ، القاهرة ،1986،ص369.

(2) د.محمود نجيب حسنى، ، شرح قانون العقوبات القسم الخاص، دار النهضة العربية ، 1978 ،ص 511.

(3) د. عمر السعيد رمضان، المرجع السابق، ص371-372.

السب، فبينما القذف لا يقوم إلا بإسناد واقعة معينة ومحددة إلى المجنى عليه فإن السب لا يلزم فيه إسناد واقعة معينة بل يكفى أن يكون موضوعه متضمناً بأى وجه من الوجوه خدشاً للشرف والإعتبار [1].

- **تعيين الواقعة :**

لا يكفى أن يسند القاذف إلى الغير أمراً شائناً وإنما يشترط أن يكون الأمر معيناً ومحدداً، فإذا كانت العبارة الشائنة المسندة إلى المجنى عليه لا تتضمن إسناد واقعة معينة فالجريمة تعتبر سباً لا قذفاً ، إذ أن تحديد وتعيين الواقعة يجعلها أقرب إلى التصديق.

ويشترط القانون فى الواقعة المسندة أن يكون من شأنها عقاب من تنسب إليه بإعتبارها جريمة ، أو إحتقاره عند أهل وطنه.

والواقعة التى تكون جريمة لا يثير أمرها صعوبة، إذ أن كل واقعة تعتبر جريمة فى حكم القانون سواء كانت جناية أو جنحة أو مخالفة يصح أن تقوم بإسنادها جريمة القذف[2].

أما الأمر الموجب للإحتقار فلم يضع له القانون تعريفاً ولم يسرد له بياناً جامعاً مانعاً ، وما كان فى وسعه أن يفعل ذلك . ذلك أن الأمور الموجبة للإحتقار لا يمكن حصرها[3].

- **تعيين المقذوف:**

يلزم بطبيعة الحال تعيين الشخص أو الأشخاص الذين تسند إليهم الواقعة الشائنة ، وليس بلازم أن يكون هذا التعيين بذكر إسم الشخص المقذوف بل يكفى تحديد شخصيته بغير ذلك من الأمارات كالزمان والمكان والمهنة وغير ذلك من معالم الشخصية[4]، أما إذا لم يمكن أو تعذر وإستحال تحديد المقذوف بحقه فلا وجود لجريمة القذف ، ويستوى أن يكون المقذوف شخصاً طبيعياً أو شخصاً معنوياً[5].

3. علانية الإسناد:

يشترط لمعاقبة القاذف أن يقع منه القذف علناً، والعلة فى ذلك أن العلنية وسيلة علم

---

(1) د.منصور السعيد ساطور.، جريمتى القذف والسب، بحث مقارن فى القانون الجنائى الوضعى والفقه الجنائى الإسلامى، بدون دار نشر، 1980،ص19.

(2) د. عمر السعيد رمضان ، المرجع السابق، ص 372.

(3) د. رمسيس بهنام، القسم الخاص فى قانون العقوبات ، دار المعارف، الطبعة الأولى، 1958، ص347 . 348.

(4) د.منصور السعيد ساطور، المرجع السابق ،ص15.

(5) راجع فى ذلك د.حسنين إبراهيم صالح عبيد ، المرجع السابق، ص203.

أفراد المجتمع بعبارات القذف وشرط لتصور إخلالها بالمكانة الإجتماعية للمجنى عليه(1).

وينص قانون العقوبات المصرى فى فى مادته 302 والتى بدورها أحالت على المادة 171 عقوبات فى تبيان صور العلانية حيث نصت المادة 171 فى فقرتها الأخيرة على :

ويعتبر القول أو الصياح علنيا إذا حصل الجهر به أو ترديده بإحدى الوسائل الميكانيكية في محفل عام أو طريق عام أو أي مكان آخر مطروق أو إذا حصل الجهريه أو ترديده بحيث يستطيع سماعه من كان في مثل ذلك الطريق أو المكان أو إذا أذيع بطريق اللاسلكي أو بأية طريقة أخرى.

ويكون الفعل أ والإيماء علنيا إذا وقع في محفل عام أو طريق عام أو في أي مكان أخر مطروق أو إذا وقع بحيث يستطيع رؤيته من كان في مثل ذلك الطريق أو المكان.

وتعتبر الكتابة والرسوم والصور الشمسية والرموز وغيرها من طرق التمثيل علنية إذا وزعت بغير تمييز على عدد من الناس أو إذا عرضت بحيث يستطيع أن يراها من يكون في الطريق العام أو أي مكان مطرق أو إذا بيعت أو عرضت للبيع في أي مكان)

ويلاحظ فى النص أن صور العلانية قد وردت على سبيل المثال لا الحصر الأمر الذى يفيد إمكانية إضافة طرق أخرى للعلانية كالإنترنت.

وقد إعتبر المشرع المصرى كذلك القذف الحاصل عن طريق التليفون قذفاً ، وتسرى عليه الأحكام الخاصة بالقذف بالرغم من عدم توافر ركن العلانية فيه.

وكذلك الحال فى قانون العقوبات الليبى حيث اعتبر المشرع الليبى العلانية متوفرة كما ورد فى المادة 16 عقوبات فقرة أولى إذا ما ارتكبت الجريمة :

أ – بطريق الصحافة أو غيرها من وسائل الدعاية أو النشر .

ب– في محل عام أو مفتوح أو معروض للجمهور وبحضور عدة أشخاص .

ج– في اجتماع لا يعد خاصاً نظراً للمكان الذي انعقد فيه أو لعدد الحاضرين أو للغرض الذي عقد من أجله .

وبناءً على ما تقدم فإن صور العلانية قد تتمثل فى القول والصياح . الفعل و الإيماء . الكتابة.

1– **علانية القول أو الصياح :** القول هو ذلك الصوت المنبعث من الفم منطوياً على كلمات

---

(1) د.محمود نجيب حسنى، المرجع السابق، ص538.

مفهومة أياً كانت اللغة التى نطق بها، ويشترك الصياح معه فى هذا المدلول ويتميز عنه فى كونه . غالبا . غير مفهوم . كالعويل والدمدمة . أو ذا دلالة عرفية معينة[1].

وتتمثل علانية القول أو الصياح فى ثلاث صور هى:

- **الجهر بالقول أو الصياح أو ترديده بإحدى الوسائل الميكانيكية فى محفل عام أو طريق عام أو أى مكان آخر مطروق** : يعنى الجهر بالقول النطق بعبارات القذف بصوت مرتفع بحيث يستطيع أن يسمعها عدد من الناس بغير تمييز ممن يوجدون فى المكان العام الذى صدرت فيه عن المتهم عباراته . أما ترديد القول بوسيلة ميكانيكية فيعنى الإستعانة بهذه الوسيلة لجعل الصوت مسموعاً فى أرجاء المكان العام[2].

  ويقصد بالمحفل العام ، الإجتماع الذى يضم عدداً كبيراً من الأفراد ويجوز لكل شخص الإنضمام إليه، ويقصد بالطريق العام كل سبيل يباح للجمهور المرور به ، أما المكان المطروق فهو كل مكان مفتوح للجمهور كدور العبادة والمتاحف العامة والمحلات التجارية[3].

- **الجهر بالقول أو الصياح فى محل خاص بحيث يستطاع سماعه من مكان عام:** والعلة من إعتبار العلنية قائمة فى هذه الصورة ، هى سماع الجمهور لعبارات القذف وحصول التشهير بالمجنى عليه ووصول ذلك إلى علم الجمهور، على الرغم من أن الوقائع المسندة إليه قد حصلت فى مكان خاص[4].

- **الإذاعة بطريق اللاسلكى أو أى طريقة أخرى:** فى هذه الفرضية تتحقق العلانية بإذاعة القول أو الصياح عن طريق جهاز اللاسلكى أو أى طريقة أخرى (كالإنترنت مثلاً) من شأنها إيصال الواقعة محل الإسناد إلى مسامع وأنظار الجمهور .

2- **علانية الفعل أو الإيماء** : نصت المادة 171 عقوبات على أن "الفعل أو الإيماء يكون علنياً إذا وقع فى محفل عام أو طريق عام أو فى أى مكان آخر مطروق أو إذا وقع بحيث يستطيع رؤيته من كان فى مثل ذلك الطريق أو المكان"

والعبرة فى تحقق علانية الفعل أو الإيماء ليست فى مجرد وقوعه فى مكان عام ، بل هى فى رؤيته أو إمكانية رؤيته لمن يكون حاضراً فى مثل ذلك المكان. فإذا صدر الفعل أو

---

(1) د.حسنين إبراهيم صالح عبيد ، المرجع السابق،ص208.

(2) د.محمود نجيب حسنى ، المرجع السابق، ص542.

(3) د.منصور السعيد ساطور، المرجع السابق، ص28.

(4) د.حسنين إبراهيم صالح عبيد ، المرجع السابق ، ص210.

الإيماء خفية بحيث لا يراه أو لايمكن أن يراه إلا من هو مقصود فلا تتحقق به العلانية ولو وقع فى محفل عام، وعلى العكس تتحقق العلانية بالفعل أو الإيماء ولو وقع فى مكان غير عام مادام يستطيع أن يراه من يكون فى الطريق العام أو أى مكان آخر مطروق(1).

3- **الكتابة** : يراد بالكتابة كل ما هو مدون بلغة مفهومة أو مستطاع فهمها، أياً كانت اللغة وأياً كانت كيفية تدوينها، فيستوى أن تكون الكتابة قد حررت باليد أو كتبت بالآلة الكاتبة أو طبعت بأية وسيلة من وسائل الطباعة(2).

وتتوافر وسائل العلانية بالكتابة إذا ما توافرت شروط ثلاثة هي:

- **الشرط الأول** : التوزيع.
- **الشرط الثاني** : العرض.
- **الشرط الثالث** : البيع او العرض للبيع.

- **الشرط الأول : التوزيع :**

هو تسليم ما هو مكتوب وتوزيعه على عدد من الأشخاص دون تمييز، بشكل مادى يتمثل فى التسليم الفعلى لا الشفوى حيث أن الشفهية لا تتحقق بها العلانية.

ولا يشترط أن يطلع على المكتوب كثيرون حيث لم يضع القانون حداً أدنى لهم ولذلك يكفى أن يطلع عليه شخصان، كما لا يشترط أن يطرح الجانى فى التداول نسخاً عديدة(3).

- **الشرط الثانى : العرض:**

طريقة أخرى تتحقق بها العلانية وهى عرض المادة التى تحتوى القذف بطريقة تمكن الآخرين من الإطلاع عليها، سواءً تم ذلك العرض فى مكان عام أو مطروق ، أو فى مكان خاص يتيح للموجود فى مكان عام من مشاهدتها.

- **الشرط الثالث : البيع أو العرض للبيع :**

يقصد بالبيع نقل الملكية نظير ثمن معين، ويتحقق فى هذه الحالة ببيع المكتوب المتضمن عبارات القذف إلى الجمهور . بغير تمييز طبعاً . أما العرض للبيع فهو إيجاب صادر عن الجانى ببيع المكتوب وذلك بشتى وسائل الدعاية أو الإعلان ، وتعد العلانية قائمة ولو كان

---

(1) د.أحمد أمين بك ، شرح قانون العقوبات المصرى ، القسم الخاص، بدون ناشر، 1949، ص117.

(2) د.أحمد أمين بك ، شرح قانون العقوبات المصرى، المرجع السابق ، ص 117.

(3) د.حسنين إبراهيم صالح عبيد ، المرجع السابق، ص212.

البيع أو العرض للبيع قد حصلا فى مكان خاص إذ أن مصدر العلانية ليس هو المكان الذى يحصل فيه البيع أو العرض ولكنه الوسيلة التى تتم بها إستفاضة مضمون الكتاب وذيوعه[1].

العلانية بأى وسيلة أخرى:

أضاف المشرع المصرى فى نص المادة 171 عبارة " أو بأى وسيلة أخرى من وسائل العلنية"

وكذلك المادة 16 ق/ع/ل نصت أن العلانية تتحقق بأى وسيلة من وسائل الدعاية والنشر الأمر الذى يمكن معه القول تحقق العلانية بغير الطرق المتقدمة و للقاضي أن يستخلص العلانية من أى طريقة تمت بها تفيد وفقاً لقناعاته تحققها.

ثانياً : الركن المعنوى لجريمة القذف: (القصد الجنائى)

القذف جريمة عمدية ، ومعنى عمدية أن الجانى يتعمد فيها إرتكاب الفعل الموجب للعقاب أو للإحتقار ، وبالتالى فهو يعلم حقيقة الفعل المرتكب ، إضافةً لإتجاه إرادته لإرتكاب هذا الفعل . وبتوافر عنصرى العلم والإرادة يكتمل القصد الجنائى لجريمة القذف.

- **العلم** : فلابد أن ينصرف إلى أركان الجريمة، ومعنى ذلك أنه يتعين علم الجانى بدلالة التعبير الذى استعمله بأن من شأنه المساس بشرف المجنى عليه والحط من قدره.فإذا جهل ذلك فإن القصد الجنائى لا يعد قائماً لديه[2].
- **الإرادة** : فتعنى إرادة الفعل وإرادة النتيجة. وإرادة الفعل تتحقق حيث يكون القول أو الإيماء أو الكتابة وليد إرادة حرة وليس إكراه أو سكر اضطرارى. أما إرادة النتيجة فتعنى إرادة النيل من سمعة المجنى عليه والحط من شرفه فى المجموعة التى يحيا فيها . والنتيجة فى القذف إذن نتيجة معنوية لا تتمثل فى أثر مادى (كالوفاة مثلاً) ولكنها تتمثل فى أثر معنوى هو التغيير الذى يلحق بالفكرة السابقة عن شخص معين فى أذهان الناس[3].

وفى ذلك قضت المحكمة العليا الليبية " أن القصد الجنائى العام يكفى لإثبات جريمة القذف ولا يؤثر فيه أن يكون القاذف حسن النية حتى يثبت القذف الموجب للعقاب"[4].

---

(1) د.حسنين إبراهيم صالح عبيد ، المرجع السابق ، ص 213.

(2) د.جلال ثروت، نظم القسم الخاص فى قانون العقوبات، منشأة المعارف، 2000، ص28.

(3) د.جلال ثروت،المرجع السابق، ص29.

(4) طعن جنائى رقم 21 / 6 ق ، بتاريخ 1961/4/22 .

عقوبة القذف:

نصت المادة 1/303 من قانون العقوبات المصرى على أنه "يعاقب على القذف بغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد عن خمسة عشرة ألف جنيه أو بإحدى هاتين العقوبتين" ، هذا فى حالة القذف البسيط أما القذف المشدد فإنه يتحقق بإحدى هذه الصور:

- القذف ضد شخص عام المادة (2/303).
- القذف عن طريق النشر فى الجرائد والمطبوعات المادة(307).
- القذف المتضمن طعناً فى الأعراض أو خدشاً لسمعة العائلات المادة(308).

أما فى ليبيا فقد نصت المادة 4 من القانون رقم (52) لسنة 1974م بشأن إقامة حد القذف على أنه (مع عدم الإخلال بحكم المادة السابعة من هذا القانون يعاقب بالجلد حداً ثمانين جلدة ، ولا تقبل له شهادة كل من ثبت عليه إرتكاب الجريمة المنصوص عليها في المادة الأولى من هذا القانون).

ويلاحظ على هذا النص أن المشرع قد قرر للقذف عقوبتين: أحداهما أصلية وهي (الجلد)، والأخرى تبعية وهي (عدم قبول الشهادة).

الفــرع الثانـــى
جريمـــــة الســـــب

تعريف السب:

يقصد بالسب كل خدش للشرف والإعتبار، فهو ذو مدلول أوسع من القذف الذي لا يتحقق إلا بإسناد واقعة تفضي إلى خدش شرف المسند إليه بما تستتبعه من عقابه أو احتقاره عند أهل وطنه[1].

أركان السب:

- ركن مادى.
- ركن معنوى.

- **الركن المادى:**

يتمثل الركن المادى فى جريمة السب، فى كل سلوك يصدر عن الجانى ويكون منطوياً بأى وجه من الوجوه على خدش لشرف المجنى عليه أو إعتباره،وبهذا يفترق السب عن القذف حيث لا يستلزم أن يكون موضوعه واقعة معينة، بل يتحقق بإسناد أى أمر يكون له هذا الشأن . وهو يتحقق بإسناد عيب معين إلى المجنى عليه : كنعته بأنه كاذب أو مقامر أو عربيد[2].

وتطبيقاً لذلك قضت المحكمة العليا " أن الفارق بين جريمة السب وجريمة التشهير هو أن التشهير يتحقق إذا حصل الإعتداء على سمعة الغير فى غيابه وكان بحضور أكثر من شخص أما إذا وقع الإعتداء فى حضور المجنى عليه فإنه يكون جريمة السب وفقاً للمادة 438 عقوبات[3].

- **الركن المعنوى:(القصد الجنائى)**

وهو إنصراف إرادة الفاعل إلى الفعل المادى المكون للجريمة كما وصفه القانون . والركن المعنوى ينهض على أساس العلم بسوء دلالة التعبير وإتجاه إرادة الجانى لإتيان هذا الفعل والنتيجة المترتبة على هذا الفعل على النحو السابق بيانه فى جريمة القذف.

والسب نوعان : سب علنى وسب غير علنى.

- **السب العلنى:**

---

(1) د.حسنين ابراهيم صالح عبيد، المرجع السابق، ص232.

(2) د.حسنين ابراهيم صالح عبيد، المرجع السابق، ص232.

(3) طعن جنائى رقم 12 / 19 ق ، بتاريخ 1973/12/18.

يقوم السب العلنى على ثلاثة أركان

- ركن مادى.
- ركن معنوى.
- ركن العلانية.

وقد سبق لنا بيان وشرح تلك الأركان لذلك نحيل عليها منعاً للتكرار.

- **السب غير العلنى:**

يتفق السب غير العلنى مع السب العلنى فى ضرورة توافر الركنين المادى والمعنوى ولا يختلف عنه إلا فى ركن العلانية.

عقوبة السب:

نصت المادة 306 من قانون العقوبات المصرى على أن" كل سب لا يشتمل على إسناد واقعة معينة بل يتضمن بأى وجه من الوجوه خدشاً للشرف والإعتبار يعقب عليه فى الأحول المبينة بالمادة 171 بالحبس مدة لا تتجاوزسنة وبغرامة لا تزيد على خمسة آلاف جنيه أو بإحدى هاتين العقوبتين". ويكون السب مشدداً فى حالة إذا ما

- ارتكب بطريق النشر فى الجرائد أو المطبوعات.
- أو إذا تضمن طعناً فى عرض الأفراد وخدشاً لسمعة العائلات.

أما قانون العقوبات الليبى فقد تناول جريمة السب فى المادة 438 بنصه:

" كل من خدش شرف شخص أو اعتباره في حضوره يعاقب بالحبس مدة لا تجاوز ستة أشهر أو بغرامة لا تجاوز خمسة وعشرين جنيهاً . تطبق العقوبة ذاتها على من ارتكب الفعل بالبرق أو التليفون أو المحررات أو الرسوم الموجهة للشخص المعتدى عليه . وتكون العقوبة الحبس لمدة لا تجاوز السنة أو الغرامة التي لا تجاوز أربعين جنيهاً إذا وقع الإعتداء بإسناد واقعة معينة".

الفــرع الثــالث

جرائــم القــذف والســب عبر الإنترنت

حددت المادة 171 و16 من قانونى العقوبات المصرى والليبى على التوالى صور العلانية والتى عرضناها بالشرح سابقاً ، ولكن نفس المادتين أضافتا أن العلانية يمكن أن تتم بأى وسيلة أخرى ، ولعله من المنطقى أن يعتبر الإنترنت وسيلة من ضمن وسائل العلانية نظراً لأن المادة المنشورة أياً كانت صورة أو مقال تكون تحت متناول أى شخص يتصفح الإنترنت دون تحديد أو تمييز أو إنتقاء لمتلقى هذه المادة. ومن الممكن إرتكاب جرائم القذف والسب عبر الإنترنت بأحد الصور التالية:

1- إنشاء مواقع على الإنترنت متخصصة فى القذف والسب:

تعمل هذه المواقع على إبراز سلبيات الشخص المستهدف ونشر أسراره، والتي قد يتم الحصول عليها بطريقة غير مشروعة بعد الدخول على جهازه، أو بتلفيق الأخبار عنه. ومن ذلك قيام شخص في دولة خليجية بإنشاء موقع ونشر صور إحدى الفتيات وهي عارية وفي أوضاع مخلة مع صديقها[1].

وفي جمهورية مصر العربية تمكنت المباحث المصرية من ضبط مهندس مصري يقوم بنشر معلومات كاذبة على إحدى مواقع الويب بهدف التشهير بعائلة مسئول مصري وإبنته. وفي واقعة مماثلة أصدرت محكمة جنح مستئأف النزهة حكماً بالحبس 6 أشهر على أحد الأشخاص قام بإنشاء موقع خاص له على شبكة الإنترنت ووضع عليه صورا إباحية مركبة عن إحدى الفتيات ومعلومات تمس شرفها وسمعتها. وفي دولة الإمارات العربية المتحدة أدانت محكمة جنح دبي أحد مشجعي كرة القدم بتهمة القذف والسب لشرطة دبي على شبكة الإنترنت ، حيث أنه أنشاء موقعا خاصا به على الشبكة تعرض فيه بالقذف والسب لشرطة دبي بزعم أنها ضربته بعد إحدى المباريات. وقضت بتغريمه ثلاثة آلاف درهم إماراتي[2].

وفى السعودية كذلك ووفقاً لنظام مكافحة الجرائم المعلوماتية تم محاكمة إثنين من المواطنين قاما بكتابة مقالات تتضمن السب والشتم والإتهامات الكاذبة فى حق شخص ثالث عن طريق أحد المنتديات الإليكترونية[3].

وتتحقق العلانية عن طريق مواقع الإنترنت كذلك ، عن طريق الصحف التى تملك مواقع

---

(1) محمد عبدالله منشاوي، جرائم الإنترنت من منظور شرعي وقانوني، بحث منشور على الإنترنت، ، راجع الموقع : http://www.minshawi.com/old/internetcrim-in%20the%20law.htm

(2) http://www.prameg.com/vb/t66778.html

(3) http://www.m3rof.com/vb/t29170.html

إليكترونية خاصة بها ، حيث أن عبارات السب والقذف تكون فى متناول كل من يتصفح موقع الصحيفة ، حيث يتوفر فيها شرط العرض للغير.

والجدير بالذكر أن بعض المواقع الإليكترونية تتيح خدمة إرسال رسائل قصيرة مجانية إلى التليفونات النقالة ، الأمرالذى أدى بالبعض لإستغلال تلك الميزة فى إرسال رسائل تحوى ألفاظاً خادشة للحياء وماسة باعتبار الشخص المستقبل لهذه الرسائل ، حيث أن هذه الخدمة لا تظهرهوية الشخص المرسل.

2- البريد الإليكترونى:

يعرف ب (E-Mail) وهوطريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات[1].

وهذا البريد الإليكترونى يستخدم كمستودع لحفظ الأوراق والمستندات الخاصة فى صندوق البريد الخاص بالمستخدم، شرط أن يتم تأمين هذا الصندوق بعدم الدخول إليه، وذلك بطرق التأمين المعروفة ومنها التشفير، وكلمات المرور password ، وغيرها من تقنيات الحماية الفنية[2].

وتعد رسائل البريد الإليكترونى المرسلة من شخص لآخر سواء كانت رسائل إليكترونية أو عن طريق الشات[3] فيما بينهم رسائل خاصة ، أى لا تتوفر فيها العلانية ، وبالتالى إذا حوت تلك الرسائل إهانة أو سباً فإننا نكون بصدد سب غير علنى.

وكذلك يمكن إعتبار جريمة القذف قد وقعت فى المثال السابق حتى فى حالة عدم تحقق العلانية، على إعتبار أن المشرع المصرى قد أقر بوقوع جريمة القذف عن طريق التليفون ، وبما أن شبكة الإنترنت قد تعتمد على شبكة الأسلاك الهاتفية فى إنشائها ، فإن القذف فى هذه الفرضية الواقع عن طريق البريد الإليكترونى يعد قذفاً عن طريق التليفون بالتبعية، وتتحقق العلانية كذلك إذا ما قام أحد الهاكرز بإقتحام البريد الإليكترونى لأحد الأشخاص ، وإطلع على مايحويه وقام بنشر الرسالة التى تحوى سباً وقذفاً على شبكة الإنترنت بحيث يتاح لكافة مستخدمى الشبكة الإطلاع علي مضمونها.

---

(1) د. خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات،بحث منشور بالموقع التالى : http://www.tashreaat.com/view_studies2.asp?id=658&std_id=99

(2) د.عبد الفتاح بيومى حجازى، الحكومة الإليكترونية ونظامها القانونى ، المجلد الأول، النظام القانونى للحكومة الاليكترونية، دار الفكر الجامعى ،2004 ،ص172.

(3) كلمة شات جذورها غربيه وهى كلمه تتماشى مع البرامج الكثيره التي حصرت تحت قالب التعارف عبر النت أو الصداقه.

وبشكل عام فإن العلانية تتحقق إذا ما تم إرسال الرسائل الإليكترونية لعدد غير محدود من الأشخاص ودون تمييز بينهم.

وكذلك فإن البريد الإليكترونى يمكن إستخدامه للدخول إلى ما يعرف بغرف الشات والدردشة، وهى عبارة عن ملتقيات جماعية لعدد من الأشخاص يلتقون فيها للتحاور والتعارف ، ويتاح فيها التحدث بالصوت والكتابة بل وبالكاميرات التى من خلالها يمكنهم رؤية بعضهم البعض ، ولكن فى أغلب الأحيان ينتهى بهم الأمر إلى تبادل السباب والشتائم ، وهو أمر تتحقق به العلانية أيضاً لأن مايحدث يشهده عدد كبير من المتواجدين بغرفة الدردشة فغرف الدردشة فى هذا المقام توازى المكان المطروق.

ومن أبرز الأمثلة على جرائم القذف والسب الواقعة عبر البريد الإليكترونى، قيام شاب فى مصر بإرسال رسائل سب وقذف فى حق مديرة إحدى الشركات السياحية وقد قام بإرسال هذه الرسالة لكافة العاملين بالشركة ومديرين كافة الفروع بقصد التشهير بها ، إنتقاماً منها بسبب رفضها تعيينه بالشركة(1).

وكذلك قيام محامى مصرى بإرسال رسائل إلكترونية تحمل عبارات سب وقذف فى حق شخص آخر وأقاربه ، الأمر الذى دعا المجنى عليه إلى التوجه إلى إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بوزارة الداخلية، حيث توصلت عمليات الفحص الفني والتقني التى قامت بها الإدارة المذكورة، إلي أن الرسائل أرسلت من جهاز كمبيوتر تبين أنه خاص بالمتهم(2).

وفى ليبيا قام أحد الأشخاص بإلتقاط صور لإحدى الفتيات مستخدماً هاتفه النقال ، وقام بإنشاء بريد إليكترونى بإسم ذات الفتاه ، ووضع صورتها على هذا البريد إضافةً إلى بعض العبارات المشينة بحقها(3).

والآن وبعد أن استعرضنا بعض جرائم القذف والسب الواقعة عن طريق الإنترنت ، فإن ثمة تساؤل يطرح نفسه فى ظل غياب نصوص تشريعية خاصة بجرائم الإنترنت ، حول إمكانية تطبيق النصوص العقابية التقليدية على مثل هذه النوعية من الجرائم.

وبخصوص الرد على هذا السؤال فإننا . وحسب ما نظنه وفقاً للمنطق صحيحاً . فإن

---

(1)http://www.nasbcom.net/vb/showthread.php?t=7208.

(2) جريدة الأهرام،العدد44692، بتاريخ 17-4-2009 ، ص12.

(3) عثمان سعيد المحيشي، ورقة عمل مقدمه إلى المنظمة العربية للتنمية الإدارية ، المؤتمر الدولي الأول لقانون الإنترنت21-25 اغسطس2005 ، منشور على الموقع.
http://www.minshawi.com/other/muhashy.htm

إعمال نصوص قانون العقوبات التقليدى واجب فى هذه الحالة ، فالقول بغير ذلك يؤدى إلى تحول الإنترنت إلى عالم غير مأمون تسوده الفوضى واللاأخلاقيات ، ويسند هذا الرأى أدلة تتمثل فى :

أن المادة 171 من قانون العقوبات المصرى قد نصت على بعض طرق العلانية على سبيل المثال لا الحصر، وأنها أضافت أن العلانية من الممكن تحققها بأى وسيلة أو طريقة أخرى.

والإنترنت . دون شك . يعتبر وسيلة فعالة تتحقق بها العلانية ، فأفعال القول أو الصياح أو الكتابة أو الصور والتوزيع والعرض المنصوص عليها فى المادة 171 من الممكن إرتكابها عبر الإنترنت وبنفس الوقع والتأثير كما ولو أنها ارتكبت بغير طريق الإنترنت .

وكذلك فيما يتعلق بالمكان المطروق المنصوص عليه ، فإن الإنترنت يعتبر مكاناً مطروقاً ، ذلك أنه من الممكن دخوله من قبل الكافة دون تمييز وتحديد.

وبشكل عام فإن طرق العلانية الواردة فى نص المادة 171 من الممكن تحققها عبر الإنترنت.

ونفس الأمر ينطبق على ما نصت عليه المادة 16 من قانون العقوبات الليبى ، حيث حددت طرق العلانية ، ونصت أن العلانية كذلك قد تتحقق بأية وسيلة أخرى ، وهو ما ينطبق على الإنترنت بنفس المعنى الذى أوردناه سابقاً.

ورغم تسليمنا بمدى أهمية تطبيق قانون العقوبات التقليدى فى مواجهة هذه الجرائم ، إلا أن ذلك ليس معناه غض الطرف والإكتفاء بقانون العقوبات كحل أوحد فى مواجهة هذه الجرائم ، فهذه الجرائم تتميز بخصائص تكنولوجية وتقنية فريدة تميزها عن غيرها من الجرائم التقليدية وتجعلها فى قالب أكبر من تلك الأخيرة ، بحيث تصبح الموازنة بين هذين النوعين . جرائم تقليدية وجرائم الإنترنت . فى الخضوع لقانون واحد ضرباً من ضروب الفراغ والقصور من الناحية التشريعية ، الأمر الذى يتطلب نصوصاً تشريعية خاصة بها.

ومن الدول العربية السباقة فى هذا المجال المملكة العربية السعودية ، بإصدارها نظام مكافحة الجرائم المعلوماتية ، حيث نصت فى مادته الثالثة الفقرة 5 المتعلقة بالتشهير بالآخرين بعقوبة السجن مدة لا تزيد على سنة أو الغرامة التى لا تزيد على خمسمائة ألف ريال.

المطلـــب الثانـــى
جرائم الإعتداء على حرمة الحياة الخاصة

بادىء ذى بدء وقبل الخوض فى جرائم الاعتداء على حرمة الحياة الخاصة، ينبغى أولاً تحديد مفهوم الحياة الخاصة ، والجدير بالذكر فى هذا المقام أنه ليس ثمة إتفاق حول مفهوم الحياة الخاصة.

فقد عرفها البعض بأنها " أحد الحقوق اللصيقة بالشخصية والتى تثبت للإنسان لمجرد كونه إنساناً(1).

وقد عرف مؤتمر (الحق فى حرمة الحياة الخاصة) الذى عقد بمدينة الإسكندرية فى عام 1987 الحق فى الحياة الخاصة بأنه " حق الشخص فى أن يحترم الغير كل ما يعد من خصوصياته مادية كانت أو معنوية أم تعلقت بحرياته على أن يتحدد ذلك بمعيار الشخص العادى وفقاً للعادات والتقاليد والنظام القانونى القائم فى المجتمع ومبادىء الشريعة الإسلامية"(2).

ولعله من الملائم أن ينحصر مفهوم الحياة الخاصة فى كل مايخص الإنسان وحده دون غيره من الناس ، الأمر الذى يوجب على الآخرين إحترام خصوصياته وعدم التطفل عليها، وعدم التدخل فيها إلا برضاه المباشر.

والحجة فى ذلك الشريعة الإسلامية الغراء خير مرجع حيث يقول تعالى (يَا أَيُّهَا الَّذِينَ آمَنُوا لا تَدْخُلُوا بُيُوتاً غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَلِكُمْ خَيْرٌ لَكُمْ لَعَلَّكُمْ تَذَكَّرُونَ {27} فَإِنْ لَمْ تَجِدُوا فِيهَا أَحَداً فَلا تَدْخُلُوهَا حَتَّى يُؤْذَنَ لَكُمْ وَإِنْ قِيلَ لَكُمْ ارْجِعُوا فَارْجِعُوا هُوَ أَزْكَى لَكُمْ وَاللَّهُ بِمَا تَعْمَلُونَ عَلِيمٌ {28}) (الآيتين 27 – 28 من سورة النور).

وقول رسولنا الكريم (لاتؤذوا المسلمين ولا تعيروهم ولا تتبعوا عوراتهم ، فإنه من تتبع عورات أخيه تتبع الله عورته ، ومن تتبع الله عورته فضحه ولو فى جوف رحله). رواه الترمذى فى البر والصلة ، باب ما جاء فى تعظيم المؤمن.

---

(1) عمر فاروق الحسينى، المشكلات الهامة المتصلة بالحاسب الآلى وأبعادها الدولية ، دراسة تحليلية ونقدية لنصوص التشريع المصرى مقارناً بالتشريع الفرنسى، الطبعة الثانية، دار النهضة العربية، 1995، ص48.

(2) أنظر د.مصطفى أحمد عبد الجواد حجازى ، الحياة الخاصة ومسئولية الصحفى ، دار الفكر العربى ، 2001/2000 ، ص52 .

الفـــرع الأول

جرائم الإعتداء على حرمة الحياة الخاصة فى قانون العقوبات

تنص المادة 309 مكرراً من قانون العقوبات المصرى على أنه: يعاقب بالحبس مدة لا تزيد على سنة كل من إعتدى على حرمة الحياة الخاصة للمواطن ، وذلك بأن إرتكب أحد الأفعال الآتية فى غير الأحوال المصرح بها قانونا أو بغير رضاء المجنى عليه :

(أ) إسترق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت فى مكان خاص أو عن طريق التليفون.

(ب) التقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص فى مكان خاص.

فإذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء إجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع ، فإن رضاء هؤلاء يكون مفترضا.

ويعاقب بالحبس الموظف العام الذى يرتكب أحد الأفعال المبينة بهذه المادة إعتماداً على سلطة وظيفته.

وكذلك نصت مادة 309 مكرر (أ) على أنه : يعاقب بالحبس كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلاً أو مستنداً متحصلا عليه بإحدى الطرق المبينة بالمادة السابقة أو كان ذلك بغير رضاء صاحب الشأن .

ويعاقب بالسجن مدة لاتزيد على خمس سنوات كل من هدد بإفشاء أمر من الأمور التى تم التحصل عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الإمتناع عنه.

ويعاقب بالحبس الموظف العام الذى يرتكب أحد الأفعال المبينة بهذه المادة إعتماداً على سلطة وظيفته. ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة او تحصل عنها ، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها.

وقد نصت المادة (45) من الدستور كذلك على الآتي :" لحياه المواطنين الخاصة حرمة يحميها القانون ، ولوسائل الإتصال حرمة وسريتها مكفولة و لا تجوز مصادرتها أو الإطلاع عليها أورقابتها إلا بأمر قضائي مسبب ولمدة محدودة وفقاً لأحكام القانون".

وكذلك نص المادة 57 بأن " كل إعتداء على الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وتكفل الدولة تعويضا عادلا لمن وقع عليه الاعتداء".

وكذلك نص قانون الصحافة رقم 96 لسنة 1996 فى مادتيه 21 ، 22 فالمادة 21 تنص على أن " لا يجوز للصحفي أو غيره أن يتعرض للحياة الخاصة للمواطنين، كما لا يجوز له أن يتناول مسلك المشتغل بالعمل العام أو الشخص ذي الصفة النيابية العامة أو المكلف بخدمة عامة إلا إذا كان التناول وثيق الصلة بأعمالهم و مستهدفا المصلحة العامة".

وقد بينت المادة 22 العقوبة المترتبة على مخالفة نص المادة 21 وهى الحبس مدة لا تزيد علي سنة و بغرامة لا تقل عن خمسة آلاف جنيه و لا تزيد علي عشرة آلاف جنيه أو بإحدى هاتين العقوبتين.

وقد نص مشروع قانون العقوبات الليبي الجديد فى المادة 334 تحت عنوان الإعتداء على حرمة الحياة الخاصة على أنه:

يعاقب بالحبس أو بالغرامة التي لا تزيد على ثلاثة آلاف دينار كل من إعتدى على حرمة الحياة الخاصة لأي شخص، وذلك بأن إرتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضا المجني عليه.

أ – إسترق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق الهاتف.

ب – إلتقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان عام أو خاص.

ويعاقب بالحبس الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة إعتماداً على وظيفته.

ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة، كما يحكم بمحو التسجيلات المتحصلة عنها أو إعدامها.

وقد تناول القانون رقم "20 لسنة1991م" بشأن تعزيز الحرية فى ليبيا حرمة الحياة الخاصة فى المادتين 15 و16 حيث نصت المادة الخامسة عشرة على أن : "سرية المراسلات مكفولة فلا يجوز مراقبتها إلا في أحوال ضيقة تقتضيها ضرورات أمن المجتمع وبعد الحصول على إذن بذلك من جهة قضائية".

وكذلك نصت المادة السادسة عشرة على أن: " للحياة الخاصة حرمة ويحظر التدخل فيها إلا إذا شكلت مساساً بالنظام والآداب العامة أوضررا بالآخرين أو إذا اشتكى احد أطرافها".

الفـــرع الثانـــى
صور الإعتداء على حرمة الحياة الخاصة فى قانون العقوبات

عدد قانون العقوبات المصرى ومشروع قانون العقوبات الليبى بعضاً من الأفعال التى تعتبر انتهاكاً لحرمة الحياة الخاصة ، حقيقةً أنه ليس من الواضح ما إذا كانت الأفعال المذكورة على سبيل الحصر أم المثال ، عموماً فإن الأفعال التى تعد إنتهاكاً لحرمة الحياة الخاصة ينحصر أغلبها فى :

1- انتهاك حرمة المحادثات الشخصية.

2- إلتقاط أو نقل الصورة.

3- إذاعة أو إستعمال التسجيل أو المستند.

أولاً : انتهاك حرمة المحادثات الشخصية:

- **ماهية المحادثات الشخصية:**

تعتبر المحادثات الشخصية وعاء تنصب فيه أسرار الحياة الخاصة للناس ، ومن هنا كان للمحادثات الشخصية حرمة لا يجوز انتهاكها باعتبارها امتداد للحياة الخاصة للناس[1].

والمحادثات الشخصية للأفراد قد تكون فى مكان خاص وكذلك من الممكن كذلك حدوثها عن طريق الهاتف.

والمكان الخاص هو المكان الذى لا يمكن دخوله إلا لأشخاص يرتبطون مع بعضهم بصلة خاصة ولا يمكن للخارج عنه أن يشاهد ما يجرى بداخله أو أن يسمعه[2].

والحصول على المحادثة الخاصة ، يتم إما باستراق السمع ، أو تسجيل الحديث ، أو نقله بدون رضاء المجنى عليه، ذلك أن الرضا الصادر من هذا الأخير يزيل الخصوصية عن حديثه.

وكذلك ينبغى توافر القصد الجنائى لدى الجانى ، بأن تتجه إرادة الفاعل لإرتكاب الفعل مع علمه بخصوصية المحادثات الشخصية وكذلك علمه بعدم رضا المجنى عليه.

---

(1) د. أحمد فتحى سرور، الوسيط فى قانون العقوبات ، القسم الخاص ، الطبعة الرابعة ، دار الطباعة الحديثة ، 1991، ص773.

(2) د. محمد زكى أبو عامر ، قانون العقوبات ، القسم الخاص ، دار الجامعة الجديدة ، 2007، ص 634.

• **العقوبة المقررة لهذه الجريمة :**

نصت المادة 309 مكرر على أن العقوبة هى الحبس مدة لا تزيد على سنة.

أما إذا ارتكب الموظف العام هذه الجريمة اعتماداً على سلطة وظيفته كانت عقوبته الحبس.

وكذلك مصادرة الأجهزة التى أستخدمت فى الجريمة ومحو التسجيلات المتحصلة عنها أو إعدامها.

أما مشروع القانون الليبى فقد نص على أن العقوبة هى الحبس أو الغرامة التي لا تزيد على ثلاثة آلاف دينار، إضافة إلى مصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة ، وكذلك محو التسجيلات المتحصلة عنها أو إعدامها.

ثانياً : إلتقاط أو نقل الصورة:

محل هذه الجريمة هو صورة شخص فى مكان خاص ، وعليه فلا تقع الجريمة إلا بتوافر شرطين أولهما أن تكون الصورة لشخص ، فلا تقع الجريمة إذا كان محلها صورة لشىء أو لمستند أو لمكان ، وثانيهما أن تكون الصورة لشخص فى مكان خاص ، فإذا كانت الصورة فى مكان عام لا تقع بالفعل الجريمة[1].

يشترط كذلك لإلتقاط أو نقل الصورة توافر عنصر القصد الجنائى بعنصريه العلم والإرادة.

أما بالنسبة لعقوبة الجريمة فهى ذات العقوبة المقررة لجريمة إنتهاك حرمة المحادثات الشخصية.

ثالثاً : إذاعة أو إستعمال التسجيل أو المستند:

يراد بإذاعة التسجيل أو المستند (ويسرى على الصورة) تمكين عدد غير محدود من الناس من العلم به والإطلاع على فحواه ، أما تسهيل الإذاعة فيراد به تقديم المساعدة لمن يقوم بالإذاعة، ويراد بالإستعمال الإنتفاع بالتسجيل أو المستند ولو فى غير علانية كمن يطلع آخر على صورة ألتقطت لفتاه فى مكان خاص ، وغالباً ما ينطوى الإستعمال على الإذاعة[2].

ويجب أن يكون التسجيل أوالمستند قد تم الحصول عليه بأحد الطرق المبينة فى المادة 309 مكرر ، وبشكل عام أن يتم ذلك دون رضا المجنى عليه.

---

(1) د. فوزية عبد الستار، شرح قانون العقوبات القسم الخاص ، الطبعة الثانية ، دار النهضة العربية ، 1988، ص647.

(2) د. أحمد فتحى سرور ، المرجع السابق، ص779.

- **العقوبة المقررة لهذه الجريمة:**

بالنسبة لقانون العقوبات المصرى فإنه يجب فى هذا الخصوص أن نفرق بين أن يقوم الجانى بإذاعة أو إستعمال التسجيل أو المستند فعلاً ، وأن يقوم بالتهديد بإفشاء ما تحصل عليه من محادثات أو صور.

ففى الحالة الأولى تكون العقوبة هى الحبس. أما فى حالة التهديد بالإفشاء فتكون العقوبة هى السجن مدة لا تزيد عن خمس سنوات، وذلك إذا كان التهديد بالإفشاء بغرض حمل شخص على القيام بعمل أو الإمتناع عنه.

وإذا ارتكبت الجريمة من قبل موظف عام اعتماداً على سلطة وظيفته كانت العقوبة السجن.

إضافة إلى مصادرة الأجهزة وغيرها مما يكون قد استخدم فى الجريمة أو تحصل عنها ، وكذلك محو التسجيلات المتحصلة عن الجريمة أو إعدامها.

أما بالنسبة لمشروع قانون العقوبات الليبى فإن العقوبة هى نفسها العقوبة المقررة لإنتهاك حرمة المحادثات الشخصية أو إلتقاط ونقل الصورة.

الفرع الثالث
الإعتداء على حرمة الحياة الخاصة عبر الإنترنت

يبرز الإعتداء على حرمة الحياة الخاصة عبر الحاسب الآلى وشبكات الإنترنت فى عدة صور أهمها :

1 - جريمة الإطلاع غير المشروع على البيانات الشخصية:

تتحقق هذه الجريمة بالإطلاع غير المشروع على أسرار الأشخاص المخزنة فى الحاسب الآلى ، مما يمثل إعتداءً على حياتهم الخاصة وإنتهاك لحرمة أسرارهم ومحل الإطلاع هنا هو بيانات ومعلومات شخصية وخاصة يريد صاحبها إبقائها سرية ، وبالتالى لا تتحقق هذه الجريمة عندما يكون الإطلاع فيها مباحاً للكافة[1].

ويشترط لوقوع هذه الجريمة أن يتم الإطلاع من شخص غير مرخص له قانوناً بالإطلاع على تلك البيانات أو المعلومات الشخصية، وعليه فلا يتصور أن يتم إرتكاب هذه الجريمة من

---

(1) أسامة أحمد المناعسة ، جلال محمد الزعبي ، صايل فاضل الهواوشة ، جرائم الحاسب الآلى والإنترنت ، دراسة تحليلية مقارنة ، الطبعة الأولى ، داروائل للنشر والتوزيع ، عمان ، 2001، ص218.

قبل شخص مصرح له بتخزين وحفظ أو تصنيف تلك البيانات والمعلومات الخاصة.

ويتحقق الركن المادى لهذه الجريمة بمجرد إطلاع الجانى على البيانات الخاصة بغيره عبر شبكة الإنترنت ، أما الركن المعنوى فيتحقق بعلمه بأنه يطلع على أسرار الغير دون رضاهم ، وإتجاه إرادته لذلك.

2 ـ جريمة جمع بيانات شخصية بدون ترخيص:

تتحقق هذه الجريمة بالجمع والتخزين لبيانات شخصية تخص أشخاصاً بعينهم ويتم هذا الجمع أو التخزين بصورة غير قانونية من أشخاص أو جهات ليس لهم الحق فى القيام بهذا الجمع أو التخزين لهذه البيانات[1].

وهذا الجمع أو التخزين للبيانات الشخصية بأساليب غير مشروعة يشكل إعتداءً وتهديداً للحياة الشخصية . ويعد من قبيل هذه الاساليب غير المشروعة مراقبة واعتراض وتفريغ وقراءة الرسائل المتبادلة عن طريق البريد الإليكترونى والتوصل بشكل غير مشروع إلى ملفات تعود لآخرين، وغير ذلك من الأساليب التى يتمكن الجانى بواسطتها من جمع بيانات بشكل غير مشروع[2].

وكذلك من الطرق التى يتم من خلالها الإطلاع على البيانات الشخصية وكذلك جمعها دون ترخيص الإعتماد على تقنية ملفات الكوكيز (Cookies) وهى عبارة عن ملفات نصية تهدف إلى جمع بعض المعلومات الشخصية بالتسلل إلى جهاز الشخص متصفح موقع الإنترنت وتقوم بنقل كافة البيانات الموجودة داخل جهازه إلى السيرفر الخاص بالموقع مما يتيح العاملين على هذه السيرفر الإطلاع على تلك المعلومات.

ومن أبرز الأمثلة المتعلقة بجمع بيانات شخصية دون ترخيص قيام مراهق من ألمانيا الإتحادية (سابقاً) ، لا يتجاوز السادسة عشر عاماً بنصب (مصائد بيانات) لإلتقاط وجمع بيانات ذات طبيعة شخصية خاصة بمستخدمى الإنترنت ، وقيامه بعمليات تلاعب وإتلاف لبعض هذه البيانات وتغيير كلمات السر التى يستخدمونها[3].

وتمثل الأفعال السابق ذكرها الركن المادى لهذه الجريمة ، أما الركن المعنوى فيتمثل فى علم الجانى بعدم مشروعية تلك الأفعال ، وإتجاه إرادته رغم ذلك لإرتكابها.

وعلى الرغم من صعوبة التمييز بين ما يعد من البيانات الشخصية وبين ما لا يعد كذلك

---

(1) د.عفيفي كامل عفيفى ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ، بدون ناشرأو تاريخ ، ص257.

(2) د.عفيفي كامل عفيفى ، المرجع السابق ، ص 258.

(3) راجع بهذا الخصوص ، محمد عبد الله أبو بكر سلامة ، المرجع السابق ، ص 189.

، إلا أن البعض يرى أن من شأن استخدام الحاسبات الآلية كبنوك للمعلومات أن يمكن الجانى من التعرف إلى السمات الشخصية التى تميز الفرد الذى تعود إليه هذه البيانات مما يمثل انتهاكاً للحياة الخاصة للشخص[1].

وتكمن الخطورة فى هذا الفعل فى إمكانية استخدام تلك المعلومات السرية ذات العلاقة بالحياة الخاصة من قبل الجانى لتحقيق أهداف غير مشروعة تتمثل فى ابتزازه للمجنى عليه وتهديده بمثل تلك المعلومات بغرض حمله على القيام بعمل أو الإمتناع عنه ، أو لغرض الحصول على أى منفعة منه.

3- جريمة التهديد بالإستغلال غير المشروع للأسرار الشخصية:

تتحقق هذه الجريمة بالتهديد بالإستغلال غير المشروع للأسرار الشخصية ، حيث يستغل مرتكب هذه الجريمة ما يحصل عليه من أسرار ذات علاقة بالحياة الشخصية للأشخاص ، ويقوم بتوظيفها لغرض تهديد أصحابها بغية الحصول على منفعة مادية كانت أم معنوية على النحو السابق ذكره.

وحتى تتحقق هذه الجريمة لابد أن تكون للجانى القدرة على تنفيذ ما هدد به والذى يتمثل فى إفشاء سر للمهدد يحرص على ألا يطلع عليه أحد . وأن يكون الجانى قادراً على ذلك بإطلاعه التام على البيانات و المعلومات التى تتميز بطابع السرية . بالإضافة لمقدرته على إفشاء تلك الأسرار متى شاء.

وفى ذلك قضت محكمة سعودية بسجن شابّ سعودي وجَلْده وتغريمه بعد اتهامه بارتكاب جريمة إلكترونية عبر الإنترنت، في حادثة هي الأولى من نوعها في البلاد بعدما ثبت أنه قام باختراق البريد الإلكتروني الخاص بفتاة سعودية، وسحب صورها الشخصية منه ، وقيامه بتهديدها بنشر تلك الصور محاولةً منه لإبتزازها[2].

وكذلك الحكم الذى أصدرته محكمة التمييز بالرياض على مواطن سعودى بالسجن 13 عاماً والجلد 1200 جلدة لإتهامه بإبتزاز نساء وتهديدهن ببث صورهن عبر الإنترنت مستغلاً عمله في أحد المراكز النسائية بإحدى المحافظات السعودية[3].

أما إذا كانت المعلومات التى بحوزة الجانى مباحة للكافة بحيث لا تتوافر فيها صفة

---

(1) د.عفيفي كامل عفيفى ، المرجع السابق ، ص 258.

(2)http://islamtoday.net/bohooth/artshow-50-105674.htm

تحت عنوان السعودية تطبق أول حكم قضائي فى جرائم الإنترنت

(3)http://download.paramegsoft.com/news-52

الخصوصية المشمولة بالحماية الجنائية فلا يحقق التهديد أثره ، كذلك لا يتحقق التهديد إذا لم يحدث أثره فى نفسية الشخص المهدد ، بمعنى أن تكون المعلومات والبيانات المهدد بها ليست ذات قيمة لديه ، أو أن إفشاؤها لن يلحق به الضرر الذى يتوقعه الجانى من جراء فعلته.

ويتحقق الركن المادى لهذه الجريمة بمجرد قيام الجانى بتهديد المجنى عليه بإفشاء بياناته الخاصة ، أما الركن المعنوى فيتمثل فى علمه بذلك الجرم وإتجاه إرادته لإرتكابه.

4 ـ جريمة الإفشاء غير المشروع للبيانات:

تعد هذه الجريمة تتمة لما قام به الجانى من إطلاع وجمع غير مشروع للبيانات الشخصية.

ويمكن أن يكون فعل الإفشاء موجهاً لشخص معين بذاته ، أو أشخاص معينين ، يرغب مرتكب الجريمة فى إخبارهم ، كما يمكن أن يكون هذا الإفشاء للسر بشكل عام ، بحيث يستطيع الجميع معرفته والعلم به ، كنشر الأسرار فى شبكة الإنترنت بحيث يستطيع أى شخص أن يطلع على هذا السر[1].

ومن ذلك ماحدث حين ألقت أجهزة الأمن المصرية القبض على عامل ديكورات قام بنشر أرقام تليفونات مديرته وبياناتها الشخصية على شبكة الإنترنت بعد قيامها بخصم نصف شهر من مرتبه[2].

ويتحقق الركن المادى لهذه الجريمة بحيازة الجانى للمعلومات الشخصية الخاصة بغيره ، وقيامه بإفشاء تلك البيانات لأشخاص لا يحق لهم الإطلاع على هذه البيانات ، أما إذا عرضت تلك البيانات لأشخاص لهم الحق فى الإطلاع عليها انتفى الركن المادى للجريمة.

أما الركن المعنوى فيتحقق بوجود عنصرى العلم والإرادة على النحو السابق ذكره. وإذا أمعنا النظر فيما تقدم نجد أنه من الصعب محاولة تطبيق النص الخاص بحماية حرمة الحياة الخاصة على الأربع حالات سالفة الذكر ، فقانون العقوبات سواء الليبى أو المصرى حصر حرمة الإنسان الخاصة فى محادثاته الخاصة وصورته فقط ، ولم يشمل بالحماية بياناته أو أسراره الأخرى ، . وإن كان المشرع المصرى قد كفلها بالحماية فى القانون المدنى وبعض التشريعات الضريبية وفى المسائل المتعلقة بالإحصاء السكانى . ولكن وفى ظل ثورة المعلومات كذلك فإن مفهوم الحياة الخاصة . وفقاً لما نظنه صحيحاً . سيتسع لكافة المحررات والمراسلات

---

(1) محمود أحمد عبابنة ، جرائم الحاسوب وأبعادها الدولية ، دار الثقافة للنشر والتوزيع ، عمان ، 2005 ، ص 221 وما بعدها.

(2) http://forums.mixolgy.net/t126490.html

الإليكترونية وكافة البيانات الشخصية الخاصة بالأفراد والموجوده على شبكة الإنترنت أو التى من الممكن تواجدها بالشبكة الأمر الذى يوجب ضرورة شمول باقى أسرار الإنسان بالحماية.

وفى المملكة العربية السعودية ، ووفقاً لنظام مكافحة الجرائم المعلوماتية فقد نص النظام المذكور فى مادته الثالثة على عقوبة السجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال ، أو بإحدى هاتين العقوبتين على كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية :

1- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلى.

2- الدخول غير المشروع لتهديد شخص أو ابتزازه ، لحمله على القيام بفعل أو الإمتناع عنه.

3- الدخول غير المشروع إلى موقع إليكترونى ، أو الدخول إلى موقع إليكترونى لتغيير تصاميم هذا الموقع.

4- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا.

5- التشهير بالآخرين ، وإلحاق الضرر بهم ، عبر وسائل تقنيات المعلومات المختلفة.

كما نص نظام مكافحة الجرائم المعلوماتية على أنه يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال ، أو بإحدى هاتين العقوبتين كل شخص يقوم بإنتاج ما من شأنه المساس بالنظام العام ، أو القيم الدينية ، أو الآداب العامة، أو حرمة الحياة الخاصة ، أو إعداده ، أو إرساله ، أو تخزينه ، عن طريق الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلى.

كما ينص نظام مكافحة جرائم المعلوماتية فى مادته السادسة على جواز الحكم بمصادرة الأجهزة ، أو البرامج ، أو الوسائل المستخدمة فى إرتكاب أى من الجرائم المنصوص عليها فى هذا النظام أو الأموال المتحصلة منها ، كما يجوز الحكم بإغلاق الموقع الإليكترونى ، أو مكان تقديم الخدمة إغلاقاً نهائياً أو مؤقتاً متى كان مصدراً لإرتكاب أى من هذه الجرائم ، وكانت الجريمة قد ارتكبت بعلم مالكه.

أما إتفاقية بودابست والموقعة فى 3001/11/23، والخاصة بالجريمة الإليكترونية ، فقد نصت فى المادة 2 على ضرورة أن تعتمد كل دولة طرف فى الإتفاقية ما قد يلزم من تدابير تشريعية فى مواجهة الجرائم التى ترتكب عن طريق الكمبيوتر، والتى يقصد بها الحصول على بيانات من كمبيوتر يخص آخرين أو بأى قصد آخر غير أمين

المطلـب الثالـث

الجرائـــم المخلـــة بالآداب العامـــة

يقصد بالآداب العامة مشاعر الشرف ومبادئ الإحتشام والذوق العام الداخل بوجدان المجتمع، أوهي مجموعة القواعد والأحكام المتعلقة بالأخلاق(1).

والآداب العامة جزء لا يتجزأ من أخلاق المجتمع ومن هنا كان الإعتداء عليها هو فى حد ذاته إعتداء على الأخلاق الإجتماعية ، وبالتالى كان لزاماً على المشرع أن يتدخل لتحديد الآداب العامة ومتى يكون الإعتداء عليها يعتبر جريمة تخرق الناموس الأخلاقى للمجتمع(2).

الفـــرع الأول

جرائم الإخلال بالآداب العامة فى قانون العقوبات

تناول المشرع المصرى الجرائم التى تمس الآداب العامة والحياء فى عدة نصوص قانونية ، حيث تناول جرائم الإخلال بالآداب العامة فى المادة 178 عقوبات. التى نصت على أن : " يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تقل عن خمسة الاف جنيه ولا تزيد على عشرة آلاف جنيه أو بإحدى هاتين العقوبتين كل من صنع أو حاز بقصد الإتجار أو التوزيع أو الإيجار أو اللصق أو العرض مطبوعات أو محفوظات أو رسومات أو إعلانات أو صوراً محفورة أو منقوشة أو رسومات يدوية أو فوتوغرافية أو إشارات رمزية أو غير ذلك من الأشياء أو الصور عامةً إذا كانت منافية للآداب العامة ".

وجريمة تحريض المارة على الفسق فى المادة 269 مكرر عقوبات والتى نصت على أن : " يعاقب بالحبس مدة لا تزيد على شهر كل من وجد فى طريق عام أو مكان مطروق يحرض المارة على الفسق بإشارات أو أقوال.......".

وكذلك جريمتى الفعل الفاضح العلنى وغير العلنى فى المادتين 278 ، 279 عقوبات حيث نصت المادة 278 على أن " كل من فعل علانية فعلاً فاضحاً مخلاً بالحياء يعاقب بالحبس مدة لا تزيد على سنة أوبغرامة لا تتجاوز ثلاثمائة جنيه ".

والمادة 279 التى نصت على أن " يعاقب بالعقوبة السابقة كل من ارتكب مع امرأة أمراً مخلاً بالحياء ولو فى غير علانية".

وجريمة التعرض لأنثى على نحو خادش بالحياء الواردة فى المادة 306 مكرر(أ) عقوبات.

---

(1) عبد المنعم حلاق ، جريدة الفداء السورية ، مقال بعنوان النظام العام والاداب العامة ، راجع الموقع http://fedaa.alwehda.gov.sy/_archive.asp?FileName=48950928920091206182233

(2) حسن حسن منصور ، جرائم الإعتداء على الأخلاق ، دار المطبوعات الجامعية ، 1985 ، ص105.

ونظراً لأن بعضاً من جرائم الإنترنت المخلة بالآداب العامة تستهدف الأطفال بالذات، فقد رأينا الإستعانة بنصوص قانون الطفل والمعدل بالقانون رقم 126 لسنة 2008 وقد نص القانون المذكور على حماية الطفل من الإنحراف وممارسته الأفعال المنافية للآداب.

وفى سبيل ذلك نصت المادة 96 الفقرة 6 على أن الطفل يعد معرضاً للخطر فى حال: " تعرض داخل الأسرة أو المدرسة أو مؤسسات الرعاية أو غيرها للتحريض على العنف أو الأعمال المنافية للآداب أو الأعمال الإباحية أو الإستغلال التجارى أوالتحرش أو الإستغلال الجنسى ......"

وكذلك نصت المادة 116 مكرر (أ) من ذات القانون على أن: " يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه كل من استورد أو صدر أو أنتج أو أعد أو عرض أو طبع أو روج أو حاز أوبث أى أعمال إباحية يشارك فيها أطفال أو تتعلق بالإستغلال الجنسى للطفل ، ويحكم بمصادرة الأدوات والآلات المستخدمة فى إرتكاب الجريمة والأموال المتحصلة منها ، وغلق الأماكن محل إرتكابها مدة لا تقل عن ستة أشهر ، وذلك كله مع عدم الإخلال بحقوق الغير حسن النية .

ومع عدم الإخلال بأى عقوبة أشد ينص عليها فى قانون آخر ، يعاقب بذات العقوبة كل من :

أ – استخدم الحاسب الآلى أو الإنترنت أو شبكات المعلومات أو الرسوم المتحركة لإعداد أو لحفظ أو لمعالجة أو لعرض أو لطباعة أو لنشر أو لترويج أنشطة أو أعمال إباحية تتعلق بتحريض الأطفال أو إستغلالهم فى الدعارة و الأعمال الإباحية أو التشهير بهم أو بيعهم.

ب – إستخدام الحاسب الآلى أو الإنترنت أو شبكات المعلومات أو الرسوم المتحركة لتحريض الأطفال على الإنحراف أو لتسخيرهم فى إرتكاب جريمة أو على القيام بأنشطة أو أعمال غير مشروعة أو منافية للآداب ولو لم تقع الجريمة فعلاً.

أما قانون العقوبات الليبى فقد تناول الجرائم الماسة بالآداب العامة فى نص المادة 421 والتى نصت على أن : " كل من إرتكب فعلاً فاضحاً في محل عام مفتوح أو معروض للجمهور يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تجاوز خمسين جنيها. وتطبق العقوبة ذاتها على من أخل بالحياء بتوزيع رسائل أو صور أو أشياء أخرى فاضحة أو بعرضها على الجمهور أو طرحها للبيع، ولا يعد شيئاً فاضحا النتاج العلمي أو الفني إلا إذا قدم لغرض غير علمي لشخص تقل سنه عن الثامنة عشرة ببيعه له أو عرضه عليه للبيع أو تيسير حصوله عليه بأية طريقة.

وكذلك نصت المادة 501 على أن: كل من قام في محل عام أو مفتوح أو معروض للجمهور بأفعال منافية للحياء يعاقب بالحبس مدة لا تجاوز شهراً أو بغرامة لا تزيد على عشرة جنيهات. وتكون العقوبة غرامة لا تجاوز خمسة جنيهات على كل من فاه بكلام مناف للحياء في محل عام أو مفتوح .

وفى سبيل حماية القصر والأحداث من التعرض للجرائم الماسة بالآداب العامة فقد وضع المشرع الليبى نص المادة 409 التى نصت على أن : " يعاقب بالحبس كل من حرض صغيراً دون الثامنة عشرة ذكراً كان أو أنثى على الفسق والفجورأو ساعده على ذلك أو مهد له ذلك أو أثاره بأية طريقة لارتكاب فعل شهواني أو ارتكبه أمامه سواء على شخص من نفس الجنس أو الجنس الآخر.

ولكن ما يهمنا فى هذا السياق هو الجرائم المنافية للآداب والمرتكبة عن طريق نشرها على شبكة الإنترنت ، وبالقياس على ما ذكرناه سابقاً فإن ما نصت عليه الماده 178 من قانون العقوبات المصرى ، والمادة 421 من قانون العقوبات الليبى ، يمكن معه تصور إنطباق كلاً من النصين على تلك الجرائم.

وتطلب القانون فى موضوع الجريمة أن ينصب على رسائل أو صور أو أشياء أخرى فاضحة ، وعبارة أشياء أخرى تفيد أن ماورد بالنص القانونى قد ورد على سبيل المثال لا الحصر، ومن الأشياء التى من الممكن إعتبارها (أشياء أخرى) الكتب والأشرطة وأفلام الفيديو والديسك والإسطوانات المضغوطة وغيره[1].

وعلى الرغم من أن المشرع قد عبر عن الرسائل والصور والأشياء بصيغة الجمع ، فإنه من الممكن تحقق الجريمة بتداول نسخة واحدة بالتتابع أو التعاقب بين عدد من الناس ، مثال ذلك تسليم صورة فاضحة إلى شخص للإطلاع عليها ثم تسليمها بذاتها إلى ثان وثالث ورابع وهكذا بالتتابع ، فهذه الافعال يتحقق بها التوزيع المعاقب عليه[2].

ويتحقق الركن المادى لهذه الجريمة بثلاث صور:

1- توزيع الاشياء الفاضحة: ويتحقق فعل التوزيع بتسليم الشىء المخل بالحياء لعدد من الناس معروفين للموزع أو غير معروفين له ، لأن علة التجريم تكمن فى الإخلال بالحياء والمساس

(1) د. فائزة يونس الباشا ، القانون الجنائى الخاص الليبى القسم الأول جرائم الإعتداء على الأشخاص ، دار النهضة العربية ، بدون تاريخ ، 267.

(2) د. إدوارد غالى الدهبى ، شرح قانون العقوبات القسم الخاص دراسة مقارنة للقانون الليبى والقوانين العربية والأجنبية ، الطبعة الثانية ، مكتبة غريب ، 1976، ص295.

بالنقاء الأخلاقى[1].

2- عرض الأشياء الفاضحة: يتحقق العرض بإتاحة الفرصة للجمهور للإطلاع على الشىء المعروض كما لو تم تعليق الصور فى ملصق بشارع عام أو أحد الحدائق أو جهة عامة يرتادها الجمهور ، أو مكن عدد من الأفراد من مشاهدة شريط فيديو أو ديسك على جهاز الحاسوب[2].

3- بيع الأشياء الفاضحة: بخلاف العرض والتوزيع الذى قد يتم بالمقابل أم بدونه ، فإن البيع الذى هو علاقة بين طرفين يستلزم بطبيعته أن يحدد من طرح سلعته للبيع ثمناً لها ، ويلزم المشترى بدفعه حالاً أم مؤجلاً ، وتقوم الجريمة بمجرد عرض السلعة للبيع أى لا يشترط لتحققها أن يتم الشراء فعلاً.

وفى هذا الخصوص قضت محكمة النقض "يتوافر القصد الجنائى فى جريمة الإخلال بالآداب العامة إذا عرض الجانى للبيع كتباً تتضمن قصصاً وعبارات فاحشة ولو كان لا يعرف القراءة والكتابة .....[3]

أما الركن الثانى لهذه الجريمة فهو العلانية ، والمقصود بها أن يأتى الجانى السلوك المادى فى مكان عام مفتوح أو معروض للجمهور.

أما بالنسبة للقصد الجنائى الخاص بهذه الجريمة ، فإن الجريمة تعد من الجرائم العمدية ، بمعنى وجوب توافر عنصرى العلم والإرادة لدى مرتكبها.

---

(1) د. فائزة يونس الباشا ، المرجع السابق ، ص269.

(2) د. فائزة يونس الباشا ، المرجع السابق ، ص269.

(3) نقض الطعن رقم 4 لسنة 20 ق ، بتاريخ 1950/1/30 ، مجموعة الربع قرن ، ص 292.

الفـــرع الثانـــى
الجرائم المخلة بالآداب العامة عبر الإنترنت

الجرائم المخلة بالآداب منتشرة على شبكة الإنترنت كانتشار النار فى الهشيم وبالتالى تكون شبكة الإنترنت جزء من هذه الجريمة سواء بإعتبارها وسيلة لإرتكابها أو محلاً لهذه الجريمة(1).

ولهذه الجريمة عدة صور حال إرتكابها على شبكة الإنترنت تتمثل فى:

1 - إنشاء المواقع المتخصصة فى نشرالإباحية والرذيلة:

وفرت شبكة الإنترنت أكثر الوسائل فعالية وجاذبية لصناعة ونشر المواد الإباحية الجنسية ، فيندرج تحت هذا البند جرائم إرتياد المواقع الإباحية والشراء منها ، والإشتراك فيها أو إنشاؤها ، وقد أصبح الإنتشار الواسع للصور والأفلام الإباحية على شبكة الإنترنت يشكل قضية ذات إهتمام عالمى فى الوقت الراهن بسبب الزيادة الهائلة فى أعداد مستخدمى الإنترنت حول العالم(2).

وقد أدى إنتشار المواقع الإباحية على شبكة الإنترنت إلى خلق مشكلة حقيقية لا يقتصر تأثيرها على مجتمع دون آخر ، وهذا ما أكده الباحث الأمريكي (Adsit) في إحدى دراساته حيث أشار إلى أن هذا الإنتشار الرهيب لهذه المواقع الإباحية صاحبه إرتفاع في جرائم الإغتصاب خاصة اغتصاب الأطفال، ناهيك عن العنف الجنسي ، وفقدان الأسرة لقيمها ومبادئها ، وتغير الشعور نحو النساء إلى الإبتذال بدلاً من الإحترام(3).

ولا شك في أن لإنتشار الجنس والإباحية الجنسية على شبكة الإنترنت إنعكاساته السلبية ، خاصة على المجتمع العربي المسلم المحافظ ، ففي إحدى الدراسات الحديثة التي أجريت على أفراد من مختلف أنحاء الوطن العربي أكدت النتائج أن 3.7 % من مرتكبي جرائم الجنس لهم إهتمام بمشاهدة الأفلام الإباحية سواء على الإنترنت أو خارجها، وأثبتت الدراسة قوة تأثير هذه الإباحيات في إرتكاب جرائم الاعتداء الجنسي من قبل مجرمي إغتصاب الإناث وهاتكي أعراض الذكور. وهذا ما أكده عالم النفس الأمريكي Edward Donnerstein من جامعة وسكوسون

---

(1) محمد عبيد الكعبى ، مرجع سابق ، ص131.

(2) محمد محمد صالح الألفى ، بحث بعنوان بعض أنماط الجرائم الأخلاقية عبر الإنترنت فى المجتمع العربى ، ص1. راجع الموقع :
http://www.eastlaws.com/Others/ViewMorafaat.aspx?ID=119

(3) د. حسين بن سعيد الغافري ، مقال بعنوان الإباحية على شبكة الإنترنت ، راجع الموقع الاليكترونى:
http://www.omanlegal.net/vb/showthread.php?t=441

بأمريكا حيث بين بأن الذين يخوضون في الدعارة والإباحية غالبا ما يؤثر ذلك في سلوكهم من حيث زيادة العنف وعدم الإكتراث لمصائب الآخرين وتقبلهم لجرائم الإغتصاب[1].

وتشير الإحصائيات إلى تصدر الولايات المتحدة لعدد الزيارات من قبل مواطنيها إلى هذه المواقع، تليها إيران ثم الإمارات العربية ومصر، ثم الكويت بالمرتبة السابعة تليها السعودية بالمركز الحادي عشر، علماً بأن هناك رقابة صارمة وحجب للمواقع الإباحية فى بعض البلدان العربية [2].

وتشير الإحصائيات كذلك أن أكثر من 28 ألف مستخدم إنترنت يتصفح مواقع إباحية في كل ثانية ، وأن 372 مستخدماً يكتبون كلمة بحث عن المواقع الإباحية في كل ثانية ، وأن الولايات المتحدة تنتج شريط فيديو إباحيا جديدا كل 39 دقيقة وأن أكثر من 3 آلاف دولار تنفق في الثانية الواحدة على المواقع والأفلام الإباحية كما يبلغ إجمالي عدد النساء من زوار المواقع الإباحية نحو 9.4 ملايين إمرأة شهريا ، و23% من زوار المواقع الإباحية هن من النساء و13% منهن اعترفن بذلك وأن 70% من النساء رفضن الإعلان عن أنشطتهن الجنسية عبر الإنترنت ، وأن17% من النساء الزائرات يكافحن إدمانهن لتصفح المواقع الإباحية[3].

وما يؤكد هذا الأمر إعتراف الشركات التى تملك تلك المواقع الإباحية بصحة تلك الإحصائيات ، فشركة (playboy) سيئة السمعة تتبجح بل وتفخر بأن 7،4 مليون زائر أسبوعياً يزور صفحات موقعها الإليكترونى الماجن ، وفى دراسة قامت بها شركة (website story) عن مواقع الدعارة على الإنترنت فوجدت أن بعض الصفحات الخليعة يزورها 034،280 زائر فى اليوم الواحد وأن صفحة واحدة فقط من هذه الصفحات إستقبلت خلال سنتين ثلاثة وأربعين مليوناً وستمائة وثلاثة عشر وخمسمائة وثمانية زوار ، وقد قام باحثون فى جامعة كارنيجى ميلون بإجراء دراسة على صور طلبت من الإنترنت فى 2000 مدينة فى 40 دولة وتبين من الدراسة أن نصف الصور المستعادة من الإنترنت هى صور خليعة وأن 5،83% من الصور المتداولة فى المجموعات الإخبارية هى صور خليعة[4].

وتأتى الولايات المتحدة في مقدمة قائمة أكثر البلدان امتلاكاً لصفحات جنسية على

---

(1) د. حسين بن سعيد الغافري ، المرجع السابق.

(2) عماد مهدى ، بحث اجتماعى بعنوان توظيف التقنية الحديثة لمعالجة ومكافحة الجرائم الأخلاقية ، راجع الموقع، http://emad-7272.maktoobblog.com

(3) عماد مهدى ، المرجع السابق.

(4) د.مشعل بن عبد الله القدهى ، المواقع الإباحية على شبكة الإنترنت ، راجع الموقع :
http:// www.minshawi.com/gadhi.htm

الشبكة بنصيب يتعدى 244.6 مليون صفحة ، تليها ألمانيا بنصيب يبلغ أكثر من 10 ملايين صفحة ثم المملكة المتحدة بنصيب 8.5 ملايين صفحة ثم أوستراليا واليابان وهولندا ثم روسيا وبولندا وأسبانيا[1].

إحصائيات عامة عن المواقع الاباحية[2] :

. يبلغ عدد المواقع الإباحية على شبكة الانترنت 4.2 ملايين موقع (12% من الإجمالي الكلي للمواقع).

. إجمالي عدد الصفحات الإباحية على الإنترنت يبلغ 420 مليون صفحة.

. 66% من المواقع الإباحية لا تحتوي على إنذار بكونها للكبار فقط.

. 25% من المواقع تحاصر زوارها عند الخروج منها (إعادة التوجيه لوصلات إباحية)

. عدد مرات البحث عن المواقع الإباحية بمحركات البحث 68 مليون طلب يوميا.

. عدد الرسائل الإلكترونية الإباحية 2.5 مليار رسالة يوميا.

. نسبة زوار المواقع الإباحية من مستخدمي الانترنت 42.7% من إجمالي زوار الشبكة.

. تبلغ نسبة تحميل المواد الإباحية عبر الانترنت 35% من إجمالي المواد المحملة.

. يبلغ عدد المواقع الإباحية التي تحتوي على مواد إباحية لأطفال أكثر من 100.000 موقع.

. يبلغ إجمالي عدد الزوار الشهري للمواقع الإباحية على الشبكة أكثر 72 مليون زائر.

. 89% من زوار غرف الدردشة يخوضون في موضوعات جنسية كنوع من أنواع التحرش.

. يفوق الدخل السنوي لصناعة الإباحية عبر الانترنت 12 مليار دولار أميركي.

. 20% من الزوارإعترفوا بدخولهم إلى المواقع الإباحية أثناء تواجدهم في العمل.

ولعله من الملائم القول بصحة إنطباق نصى المادتين 178 ، و421 من قانونى العقوبات المصرى ثم الليبى على التوالى على مثل هذه الجرائم ، والعلة فى ذلك أن المواد التى تحويها المواقع الإباحية (سواءً كانت صوراً أو أفلام أو دعاية) تنتشر عن طريق العرض على مستخدمى الإنترنت ، أوالتوزيع وذلك بإرسال رسائل تحوى عناوين هذه المواقع للبريد الإليكترونى

(1) عماد مهدى ، المرجع السابق.

(2) راجع بخصوص هذه الإحصائية ، عماد مهدى ، المرجع السابق.

الخاص بالمستخدم لجذبه ومحاولة إقناعه بالولوج لهذه المواقع وهو ما يعد تحريضاً على الفسق كذلك ، والصورة الأخيرة هى البيع ، حيث تقوم هذه المواقع الإباحية بتقديم بعض خدماتها مقابل بعض المبالغ المالية ، والأفعال سالفة الذكرتشكل الركن المادى فى الجرائم المنافية للآداب العامة، وذلك مع الأخذ فى الإعتبار رغبة مستخدم الإنترنت الذى يحدد ما إذا كان ينتوى مطالعة مثل هذه المواقع أم لا.

2 ـ الإستغلال الجنسى للأطفال:

يقصد بالاستغلال الجنسي للأطفال، تصوير أي طفل بأية وسيلة كانت، يمارس ممارسة حقيقية أو بالمحاكاة أنشطة جنسية صريحة، أو أي تصوير للأعضاء الجنسية لإشباع الرغبة الجنسية أساساً، ويعتبر معتدياً ولو بشكل غير مباشر، أي شخص يطالع صوراً إباحية للأطفال أو يحتفظ بها. وعندما تنشر تلك الصور على الإنترنت، تصحّ تسميتها "بورنو الأطفال[1].

وإنتشار الإباحية على شبكة الإنترنت له مخاطره على الأطفال والتي تبرز من خلال ثلاثة مخاوف رئيسة : تتمثل الأولي في قدرة الأطفال على الوصول وبسهولة إلى المواقع الإباحية ، والثانية تتمثل في كون العاملين في مجال دعارة الأطفال وجدوا شبكة الإنترنت مكاناً مناسباً لعرض منتجاتهم من المواد والأفلام الخاصة بهذه الدعارة ، والثالثة تتمثل في أن الأشخاص الشاذين المنجذبين للأطفال وجدوا في خدمة الرسائل الإلكترونية والتخاطب عبر غرف الدردشة ضالتهم في إستدراج ضحايهم من الأطفال[2].

ويتحقق الإستغلال الجنسى للأطفال عبر الإنترنت بعدة صور تتمثل فى:[3]

. حض وتحريض القاصرين على أنشطة جنسية غير مشروعة عبر الوسائل الالكترونية.

. التحرش الجنسي بالقاصرين عبر الكمبيوتر والوسائل التقنية ونشر وتسهيل نشر وإستضافة المواد الفاحشة عبر الإنترنت بوجه عام وللقاصرين تحديداً.

. نشرالفحش والمساس بالحياء(هتك العرض بالنظر)عبرالإنترنت وتصويرأوإظهارالقاصرين ضمن أنشطة جنسية.

---

(1) ليال كيوان، تحقيق بعنوان الاستغلال الجنسي للأطفال عبر الانترنت أو "بورنو الأطفال" ، جريدة النهار اللبنانية ، راجع الموقع : http://www.annahar.com بتاريخ 17 /5 /2009.

(2) د. حسين بن سعيد الغافري ، المرجع السابق.

(3) المحامى يونس عرب ، جرائم الكمبيوتر والإنترنت المعنى والخصائص والصور وإستراتيجية المواجهة القانونية ، المرجع السابق ، ص49.

وأظهرت دراسة لوزارة العدل الأمريكية تعرض طفل من كل سبعة أطفال من مستخدمي الإنترنت لإغواء جنسي، وإضطرار واحد من كل ثلاثة إلى مشاهدة مواد ذات طابع فاضح، كما تم التحرش جنسياً بطفل من بين كل 11 طفل[1].

وحسب تقارير دولية ، من بينها تقرير صادر عن " المركز القومي الأمريكي للأطفال المختطفين والمفقودين" ، إرتفعت حالات إستغلال الأطفال جنسياً عبر شبكة الإنترنت حول العالم بشكل كبير. بحيث تزايد عدد المواقع الإباحية لإستغلال الأطفال بنسبة 400 % بين سنة 2004 وسنة 2005، كما أن أكبر شريحة لمشاهدي البورنوغرافيا في الإنترنت هم فئة القاصرين الذين تتراوح أعمارهم ما بين 12 و17 سنة [2].

وقدرت مجلة" إنترنيت فيلتر" دخل التجارة الخاصة بالاستغلال الجنسي للأطفال بـ 3 مليار دولار سنة2005 ، وأظهرت العديد من الدراسات، أن المنتديات الإلكترونية وخطوط الهواتف المفتوحة ونوادي المناقشات تمثل ثلاث وسائل سهلة لدخول مواقع الإنترنت المتخصصة في الصور الخلاعية التي تستخدم الأطفال جنسياً[3].

ويحصل "بورنو الأطفال" عندما تقوم مواقع إباحية على الانترنت ببثّ صور أطفال ضحايا الإعتداء الجنسي، أو بعرض صور فيديو لقاصرين أثناء تعرّضهم لإعتداء جنسي من بالغين، والمعتدون يشكلون شبكة، ويتعرفون إلى بعضهم البعض ويتواصلون بغية تبادل الصور والأفلام الإباحية، وأسباب ممارسة تلك الأعمال متعددة، منها الإقتصادي والإجتماعي والإنساني. ومن بين أسباب إرتكاب تلك الجرائم كذلك ، هوإستخدام هذه المواد ونشرها ،أو بدافع الهواية أو الرغبة في تجميع الصور الاباحية. ومهما تكن الأسباب، يُلاحق عناصر الشرطة المجرمين عبر الإنترنت من خلال كشف الـ IP address الخاص بكل مستخدم، وفي حال كان المشتبه به مقيماً في بلد آخر يتم التبليغ عنه لشرطة بلده ، ولتفعيل عملية المكافحة توحدت الجهود الدولية بين المؤسسات العامة والخاصة المعنية، وقامت منظمة International Center of Missing Exploitation Children الممولة من شركة "مايكروسوفت"، بوضع برامج خاصة في تصرف أجهزة الشرطة على إمتداد دول العالم، من شأنها الكشف عن المجرمين بالإستناد إلى قاعدة بيانات تحتوي على الكثير من الصور وأفلام الفيديو والرسومات والكتابات تعرف بـ "بورنو

---

(1) راجع الموقع :
http://lattakia.org/ShowArticle.aspx?ID=212&AspxAutoDetectCookieSupport=1

(2) مقال بعنوان جرائم الإنترنيت التي تستهدف القاصرين ، راجع الموقع ،
http://www.jeunessearabe.info/article.php3?id_article=580

(3) مقال بعنوان جرائم الإنترنيت التي تستهدف القاصرين ، المرجع السابق.

الأطفال"، توزع عبر الشبكة العنكبوتية ويستخدمها مرتكبو جرائم الإعتداء على الأطفال في الفضاء السيبراني(1).

وفى هذا السياق واجه القضاء اللبناني في العام 2000 قضية من هذا النوع حيث تمكنت السلطات الأمنية اللبنانية بالتعاون مع الإنتربول من توقيف شخص لبناني كان يبثّ وينشر صوراً إباحية لأطفال عبر الإنترنت(2).

إحصائيات خاصة بجرائم الإستغلال الجنسى للأطفال عبر الإنترنت(3) :

. يبلغ متوسط عمر الأطفال الذين يتعرضون للمواد الإباحية لأول مرة 11 عاما.

. متوسط عمر الأطفال الأكثر إعتيادا على الدخول إلى تلك المواقع من سن 15 إلى سن 17.

. 40% من الأطفال لا يترددون في ذكر بياناتهم الشخصية والعائلية أثناء إستخدامهم للإنترنت سواء عن طريق البريد الإليكتروني أو غرف الدردشة.

. ما يقرب من 26 شخصية كارتونية محببة إلى الأطفال تستغل لإصطيادهم إلى المواقع الجنسية.

. 1 من 4 نساء يشتكين من تعرض أطفالهن للإستغلال الجنسي عبر الإنترنت.

. أكثر من 20000 صورة مخلة لأطفال تبث أسبوعيا على الإنترنت.

. 1 من 5 أطفال تعرض للتحرش الجنسي من قبل شواذ أثناء تواجده بغرف المحادثة 25% ممن تعرضوا لذلك قاموا بإبلاغ أولياء أمورهم.

ومما سبق عرضه نجد أن جرائم الإستغلال الجنسى للأطفال تحوى خليطاً من الجرائم المنصوص عليها فى نص المادة 178 ، وكذلك جرائم التحريض على الفسق فى المادة 269 مكرر وجريمة االفعل الفاضح العلنى فى المادة 278 ، فالمادة 178 تعاقب على صناعة أو حيازة أو تجارة الصور أو الرسومات المنافية للآداب العامة وهو ما يمكن إنطباقه حال تداول الصور الفاضحة الخاصة بالقصر والسعى إلى ترويجها وتوزيعها سواء بقصد الإتجار بها أم مجرد توزيعها دون مقابل على شبكة الإنترنت ، أما بالنسبة للنص العقابى الخاص بالتحريض

---

(1) ليالى كيوان ، المرجع السابق.

(2) د.نضال الشاعر، حماية الأطفال من سوء إستخدام الإنترنت وجرائم المعلوماتية ، مداخلة ضمن مؤتمر تشريعات الطفولة والعائلة في لبنان في إطار القواعد الدستورية والحقوقية ، 2006/6/25، ص5.

(3) راجع بخصوص هذه الإحصائية ، عماد مهدى ، المرجع السابق.

على الفسق فيمكن تطبيقه على هذه الجرائم ، لأن الإستغلال الجنسى للأطفال يبدأ بفكرة الترويج وتهيئة هذا الأمر للقصر وإغرائهم للإقبال عليه وهو ما يوازى التحريض ، أما بالنسبة لنص المادة 278 وهو الخاص بالفعل الفاضح فإنطباقه أمر لا يختلف عليه إثنان.

والجدير بالذكر أن المادتين 269 ، و278 إشترطتا العلانية وهو ما يعزز إمكانية تطبيق كلاً من المادتين فأبرز ما يتميز به الإنترنت هو العلانية.

أما قانون الطفل وفى نص المادة 116 مكرر(أ) منه . ووفقاً لما نظنه صحيحاً . فهى المادة الأصل من حيث التطبيق على هذه الجرائم ، لأنها نصت صراحة على إستغلال الطفل جنسياً من خلال الحاسب الآلى أو شبكة الإنترنت.

أما قانون العقوبات الليبى فإن نص المادة 409 . وفقاً للمنطق . يكون جدير بالتطبيق فى هذه الحالة لأنه نص صراحة على حماية القصر من إرتكاب أى فعل شهوانى أو التمهيد له.

أما المادتين 421 و501 فيمكن بالقياس على ما ذكرناه بالنسبة لمواد القانون المصرى تطبيقهما باعتبار الفعل فعلاً فاضحاً و مخلاً بالآداب العامة.

ووفقاً للمادة السادسة من نظام مكافحة جرائم المعلوماتية بالمملكة العربية السعودية ، فإن العقوبة هى السجن لمدة لاتزيد على خمس سنوات والغرامة التى لا تزيد على ثلاثة ملايين ريال ، أو إحدى هاتين العقوبتين، فى حال إرتكاب الجرائم الآتى ذكرها:

1. إنتاج ما من شأنه المساس بالنظام العام ، أو القيم الدينية ، أو الآداب العامة ، أو حرمة الحياة الخاصة ، أو إعداده ، أو إرساله ، أو تخزينه عن طريق الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلى.
2. إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية ، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها.

وقد سعى المجتمع الدولي للتدخل لوقف هذا التدفق للإباحية، الذي يزداد بإزدياد أعداد مستخدمي الشبكة وقد تمثلت هذه المساعي بعقد المؤتمر الدولي لمكافحة الاستغلال الجنسي للأطفال عام 1999 بفيينا ، وكان يهدف إلى توعية المستخدمين لمواجهة الإستغلال الجنسي للأطفال عبر الإنترنت، حيث أكد المؤتمر على مبدأ أساسي يتمثل في تدعيم التعاون الدولي في مكافحة الإستغلال الجنسي للأطفال عبر الإنترنت، وذلك من خلال تكثيفه للجهود الدولية في الأخذ بالمبادئ التي تؤكد وتؤطر هذا المبدأ من خلال عدة توصيات، تتمثل في:

أولاً : تشجيع وضع قواعد للسلوك من قبل مزودي خدمة الانترنت.

ثانيا : تشجيع إنشاء خطوط ساخنة للمواطنين للإبلاغ عن المواقع الإباحية للأطفال عبر

الانترنت.

ثالثاً: ضرورة محاربة الإستغلال التجاري للأطفال على الانترنت، مما يتطلب تدخل المشرع الوطني لتجريم الجنسية على الإنترنت، وذلك تحت إطار الاتفاقية الدولية المتعلقة بحماية الطفل.

رابعاً: تدعيم التعاون الدولي في مجال مكافحة جرائم الاستغلال الجنسي للأطفال من خلال إنشاء وحدات خاصة لمكافحة هذه الجرائم وإعداد برنامج تدريب خاص للتأهيل في هذا المجال

خامساً : يتعين على الدول المختلفة أن تضع قواعد دنيا تتناول تعريفاً وتحدياً مقارباً لهذه الجريمة، بحيث يؤخذ في عين الإعتبار الحيازة العمدية لصور الأطفال، وإنتاج وتوزيع، وإستيراد وتصدير ونقل صور الأطفال الإباحية والاعلان عنها بطريق الكمبيوتر أو وسائل التخزين الالكتروني واعتبارها من الجرائم المعاقب عليها.

سادساً : من الناحية الإجرائية ، يتعين إتخاذ كافة الإجراءات الكفيلة للمحافظة على البيانات المتحفظ عليها ، بما فيها البيانات الموجودة تحت يد مزود الخدمة – ولو كان في بلد آخر– مع الأخذ بعين الإعتبار المشكلات الخاصة بالتخزين وحجمه والأوامر القضائية ومقتضيات حماية البيانات ، التي قد تكون محلاً للمطالبة بتعاون متبادل بشأن كل تفتيش أو قبض أو إفشاء لمحتوى هذه البيانات كما أنه يتعين اتخاذ إجراءات مشتركة تسمح بتجاوز الحدود لتفتيش وضبط أجهزة الكمبيوتر ، بالإضافة الى إقامة وسائل الإتصال لتحقيق التعاون الدولي في هذا المجال(1).

وعلى المستوى الأوروبي ، أطلق الإتحاد الأوروبي ورقة إتصالات في المحتوى غير الشرعي والضار، مع ورقة سميت (بالورقة الخضراء) لحماية القاصرين وشرف الإنسان وإعتباره في المواد السمع بصرية وخدمات المعلومات، وذلك في عام 1996 ، حيث تضمنت حلولاً أعتمدت من قبل مجلس وزراء الإتصالات ، وتتعلق بنشر المحتوى غير الشرعي على الإنترنت خصوصاً ما يتعلق بدعارة الأطفال. وقد إعتمد البرلمان الأوروبي الحلول التي أقرها التقرير حول التفويض الأوروبي في الإتصال في عام 1997 ، ومنها ما ذهبت إليه الورقة الخضراء إلى ضرورة إختيار التحديات التي تواجه المجتمع ، والخارجة عن السيطرة نتيجة التطورات السريعة في المواد السمع بصرية وخدمات المعلومات في شتى أنحاء العالم، وقد أعطت للشرطة الحق في

---

(1) راجع بخصوص هذا المؤتمر د. معتز محيي عبد الحميد ، مقال بعنوان الإستغلال الجنسي للأطفال ، راجع الموقع الخاص بجريدة الصباح العراقية ،
http://www.alsabaah.com/paper.php?source=akbar&mlf=interpage&sid=17059

إتخاذ أثر فوري للتعامل مع المحتوى غير الشرعي على الإنترنت[1].

وقد نصت كذلك إتفاقية بودابست على الجرائم المتعلقة بالصور الفاضحة للأطفال فى المادة 9 فقرة 1، حيث أوصت بضرورة قيام كل دولة طرف فى الإتفاقية بإتخاذ التدابير التى من شأنها تجريم الأفعال والسلوكيات الآتى ذكرها:

أ . إنتاج صور فاضحة للأطفال بغرض توزيعها عبر منظومة كمبيوتر.

ب . عرض أو توفير صور فاضحة للأطفال عبر منظومة كمبيوتر.

جـ . توزيع أو بث صور فاضحة للأطفال عبر منظومة الكمبيوتر.

د . الحصول على صور فاضحة للاطفال عبر منظومة كمبيوتر لصالح الشخص ذاته أو لصالح الغير.

هـ . حيازة صور الأطفال الفاضحة داخل منظومة كمبيوتر أو بوسيط تخزين بيانات كمبيوتر.

وقد بينت المادة 9 فى فقرتها الثانية أن المقصود بصور الأطفال الفاضحة هى الصور التى تبين القاصر الذى ينشغل بارتكاب سلوك جنسى صريح أو يبدو أنه كذلك ، وعرفت فى فقرتها الثالثة القاصر بأنه من يقل سنه عن 18 عاماً.

(1) د. معتز محيي عبد الحميد ، المرجع السابق.

المبحـــث الثانـــى
الجرائم المستحدثة المرتكبة بواسطة الإنترنت

المقصود هنا بالجرائم المستحدثة أن بعضاً من الجرائم التقليدية أصبحت ترتكب بأساليب حديثة أو أكثر إبتكاراً من ذى قبل ، وكذلك قد يقصد بالجرائم المستحدثة ظهور نوعية جديدة من الجرائم مرتبطة كلياً بتقنية الإنترنت ، وقد أصبحت هذه الظواهر الإجرامية المستحدثة تتطور وتتبدل ويتزايد عددها بمرور الوقت ، وسنتناول بالبحث بعضاً من هذه الجرائم فى المطالب التالية:

المطلب الأول : الجرائم الواقعة على التجارة الإليكترونية.

المطلب الثانى : جرائم الإتلاف المعلوماتى.

المطلب الثالث : جرائم غسيل الأموال عبر الإنترنت.

المطلـــب الأول
الجرائم الواقعة على التجارة الإليكترونية

من إنعكاسات إستخدام الحاسب الآلى وإنتشاره على نحو واسع فى حياتنا ظهور فكرة التجارة الإليكترونية ، وهذه التجارة تعتمد على وسائل إليكترونية بما فيها الحاسب الآلى وشبكة الإنترنت لإتمامها. ولعل الصورة الشائعة لهذه التجارة صورة إبرام العقد عن طريق الإنترنت أو كما يطلق عليه التعاقد عن بعد(1).

ويمكن فى أغلب الاحوال إبرام عقد البيع أو الشراء عن طريق الإتصال المباشر بين المتعاقدين بطريق الإنترنت وسداد قيمة السلعة أو الخدمة بطريق التحويلات البنكية أو بطريق بطاقات الإئتمان أو بأى طريق آخر يتم تحديده بين أطراف العقد(2).

الفرع الأول
تعريف التجارة الإليكترونية

عرف توجيه البرلمان والمجلس الأوروبى رقم31 لسنة 2000 الصادر فى 8 يونيو 2000 ، الإتصال التجارى فى مادته الثانية بأنه كل شكل من أشكال الإتصال يستهدف تسويق بصورة مباشرة أو غير مباشرة بضائع أو خدمات أو صورة مشروع أو منظمة أو شخص يباشر نشاط تجارى أو صناعى أو حرفى أو يقوم بمهنة منظمة(3).

- **سمات التجارة الإلكترونية(4) :**

1. عدم وجود علاقة مباشرة بين طرفي العملية التجارية حيث يتم التلاقي بينهما من خلال شبكة الاتصالات (أي التعامل بين العملاء يكون عن بعد).

2 . هذا النوع من التجارة يؤمن إمكانية التفاعل مع مصادر متعددة في وقت واحد ، حيث يستطيع التعامل مع عدد لا نهائي من الزبائن فى نفس الوقت.

3-إمكانية تنفيذ وإنجاز كل المعاملات التي تخص نشاط العملية التجارية بما فيها تسليم السلع

---

(1) د.عبد الفتاح بيومى حجازى ، النظام القانونى لحماية التجارة الإليكترونية ، المجلد الأول: نظام التجارة الإليكترونية وحمايتها مدنياً ، الطبعة الأولى، دار الفكر الجامعى ، 2002، ص9.

(2) د. مدحت عبد الحليم رمضان ، الحماية الجنائية للتجارة الإليكترونية دراسة مقارنة ، دار النهضة العربية ، بدون تاريخ ، ص3.

(3) د. مدحت عبد الحليم رمضان ، المرجع السابق ، ص15.

(4) د. قاسم النعيمى ، بحث بعنوان التجارة الإليكترونية بين الواقع والحقيقة ، ص7 ، منشور بالموقع jps-dir.com/Forum/uploads/1364/qaseem.doc

الغير مادية على الشبكة (مثل البرامج والتصاميم وغيرها...).

- **كيفية التعاقد عبر شبكة الإنترنت:**

للتعاقد بطريق الإنترنت عدة طرق من أهمها وأكثرها انتشاراً:

1. **التعاقد عبر شبكة المواقع (web):** وذلك بأن يلج المستخدم الموقع الإليكترونى الذى يحتوى على عرض للسلع التجارية المعروضة للبيع ويختار مايشاء منها، ثم بعد ذلك تتم عملية البيع والشراء وفق الشروط التى يحددها الموقع ، والتى من ضمنها تحديد طرق الدفع والتسليم ومدة ضمان المنتج وما إلى ذلك.

2. **التعاقد عبر البريد الإلكتروني (Email):** يتم التعاقد عبر البريد الإليكترونى بقيام الشركات التجارية والتى تملك مواقع إليكترونية بإرسال رسائل بريدية إلى عدد كبير من مستخدمى الإنترنت ، تعرض فيها بضائعها وسلعها بغية إقناعهم شراء أحد منتجاتها وهو ما يعتبر إيجاب منها أو دعوة للتعاقد ، وتحوى كذلك تلك الرسائل تبيان طريقة التعاقد والدفع ومميزات المنتج.

- **طرق الدفع والسداد الإليكترونى:**

بالنسبة للدفع الإليكترونى فإنه يتم إستخدام ما يعرف بالنقود الإليكترونية كوسيلة للوفاء أو للدفع

وقد عرف البنك المركزي الأوروبي النقود الإليكترونية بأنها مخزون إليكتروني لقيمة نقدية على وسيلة تقنية يستخدم بصورة شائعة للقيام بمدفوعات لمتعهدين غير من أصدرها، دون الحاجة إلى وجود حساب بنكي عند إجراء الصفقة وتستخدم كأداة محمولة مدفوعة مقدماً[1].

- **أشكال النقود الإلكترونية[2]:**

1 – **البطاقات سابقة الدفع Prepaid Cards:** ويتم بموجب هذه الوسيلة تخزين القيمة النقدية على شريحة إليكترونية مثبتة على بطاقة بلاستيكية. وتأخذ هذه البطاقات صوراً متعددة. وأبسط هذه الأشكال هي البطاقات التي يسجل عليها القيمة النقدية الأصلية والمبلغ الذي تم إنفاقه، ومن أمثلتها البطاقات الذكية Smart Cards المنتشرة في الولايات المتحدة الأمريكية.

---

(1) د. محمد إبراهيم محمود الشافعى ، مقال بعنوان النقود الإلكترونية (ماهيتها، مخاطرها وتنظيمها القانوني) ، متوافر بالموقع : http://www.manqol.com/topic/?t=7651

(2) د. محمد إبراهيم محمود الشافعى ، المرجع السابق.

2 – **القرص الصلب:** ويتم تخزين النقود هنا على القرص الصلب للكمبيوتر الشخصي ليقوم الشخص بإستخدامها في شراء ما يرغب فيه من السلع والخدمات من خلال شبكة الإنترنت.

3 . **البطاقات الإئتمانية Credit Cards: وتستخدم** هذه البطاقات كأداة ضمان ، حيث تصدرها البنوك فى حدود مبالغ معينة ، ويقوم البنك بإستيفاء نسبة عمولة محددة عند كل إستخدام للبطاقة ، ومن أمثلتها بطاقة الفيزا والماستر كارد وأميركان إكسبريس(1).

الفـــرع الثانـــى

صـور الإعتــداء علـى التجـارة الإليكترونيـة

تتعدد وتتنوع الجرائم الواقعة على التجارة الإليكترونية ، و ينحصر أغلبها فى:

- الإعتداء على التوقيع الإليكتروني.
- السطو على أرقام البطاقات الإئتمانية.
- الإعتداء على حقول الإنترنت وأسماء الدومين.

أولاً : الإعتداء على التوقيع الإليكتروني:

التوقيع بوجه عام ما هو إلا وسيلة يعبر بها شخص ما عن إرادته في الإلتزام بتصرف قانوني معين ويستعمل مصطلح التوقيع بمعنيين : الأول ينصرف إلى فعل أو عملية التوقيع ذاتها أي واقعة وضع التوقيع على مستند يحتوى على معلومات معينة، والثاني ينصرف إلى العلامة أو الإشارة التي تسمح بتمييز شخص الموقع(2).

وبالتالي فإن للتوقيع دورا هاماً من ثلاثة جوانب فهو من جهة يحدد شخصية الموقع ومن جهة أخرى يعبر عن إرادته في إلتزامه بمضمون الوثيقة ، وإقراره لها ، ومن جهة ثالثة يعد دليل على حضور أطراف التصرف وقت التوقيع أو حضور من يمثلهم قانوناً أو إتفاقاً(3).

ومع التقدم التكنولوجي المعاصر في وسائل الإتصال ونقل المعلومات ، ظهرت طرق

---

(1) د. سليمان أحمد فضل ، المرجع السابق ، ص 158.

(2) د. محمد المرسى زهرة ، الدليل الكتابى وحجية مخرجات الكمبيوتر فى الإثبات فى المواد المدنية والتجارية ، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت ، كلية الشريعة والقانون ، جامعة الإمارات العربية المتحدة ، الفترة من 1 . 3 /5 /2000 ، ص114.

(3) د. سعيد عبد اللطيف حسن ، إثبات جرائم الكمبيوتر والمرتكبة عبر الإنترنت ، دار النهضة العربية ، 1999 ، ص244.

ووسائل حديثة في التعامل لا تتفق تماما مع فكرة التوقيع بالمفهوم التقليدي ، فمعظم المعاملات المالية والتجارية أصبحت تتم إليكترونيا ، وبالتالي لم تعد الوسيلة التقليدية في إثبات التصرفات القانونية ملائمة للتعاقدات الحديثة التي تتم في الشكل الإليكتروني ، من هنا كان ظهور التوقيع الإليكتروني ليكون بديلا عن التوقيع التقليدي ليتوافق وطبيعة التعاقدات القانونية والعقود التي تتم بإستخدام الوسائل والأجهزة الإليكترونية الحديثة [1].

- **تعريف التوقيع الإليكترونى:**

عرف القانون النموذجي بشأن التوقيعات الالكترونية الذي وضعته لجنة الأمم المتحدة للقانون التجاري الدولي (الأونسيترال) فى العام 2001 التوقيع الإليكتروني بأنه بيانات في شكل إليكتروني مدرجة في رسالة بيانات، أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تُستخدم لتعيين هوية الموّقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموّقع على المعلومات الواردة في رسالة البيانات.

- **أشكال التوقيع الإليكترونى:**

1 . التوقيع الرقمى أو الكودى:

هو عدة أرقام يتم تركيبها لتكون فى النهاية كودا يتم التوقيع به ، ويستخدم هذا فى التعاملات البنكية والمراسلات الإليكترونية التى تتم بين التجار أو بين الشركات وبعضها، ومثال لذلك بطاقة الإئتمان التى تحتوى على رقم سرى لا يعرفه سوى العميل.

2 . التوقيع بالقلم الإليكتروني:

هنا يقوم مرسل الرسالة بكتابة توقيعه الشخصى باستخدام قلم إليكتروني خاص على شاشة الحاسب الآلى عن طريق برنامج معين ويقوم هذا البرنامج بإلتقاط التوقيع والتحقق من صحته.

3 . التوقيع الشخصى:

يقوم على أساس التحقق من شخصية المتعامل بالاعتماد على الصفات الجسمانية للأفراد مثل البصمة الشخصية، مسح العين البشرية، التعرف على الوجه البشرى، خواص اليد البشرية، التحقق من نبرة الصوت.

وتعد من أكثر التوقيعات شيوعاً هذه التوقيعات الرقمية القائمة على ترميز المفاتيح ،

([1]) د. حسين بن سعيد الغافرى ، بحث بعنوان الجرائم الواقعة على التجارة الإليكترونية ، ص3، راجع الموقع :
http://www.eastlaws.com/Others/ViewMorafaat.aspx?ID=4

مابين عام وخاص فالأولى تسمح بقراءة الرسالة دون إستطاعة إدخال أى تعديل عليها ، فإذا وافق المعنى بها على مضمونها وأراد إبداء قبوله بشأنها وضع توقيعه من خلال مفتاحه الخاص عليها ، وإعادتها إلى مرسلها مذيلة بتوقيعه الإليكترونى وتعتمد هذه المفاتيح فى الأساس على تحويل المحرر المكتوب من نمط الكتابة الرياضية إلى معادلة رياضية ، وتحويل التوقيع إلى أرقام ، فبإضافة التوقيع إلى المحرر عن طريق الأرقام يستطيع الشخص قراءة المحرر والتصرف فيه ، ولا يستطيع الغير التصرف فيه إلا عن طريق هذه الأرقام[1].

وبإستطاعة أى شخص الحصول على التوقيع الإليكترونى بأشكاله المتعددة ، وذلك عن طريق التقدم إلى إحدى الهيئات المتخصصة فى إصدار هذه الشهادات والمنتشرة على شبكة الإنترنت ، وذلك مقابل مبلغ معين من المال سنوياً ، وتتم مراجعة الأوراق والمستندات ومطابقة الهوية بواسطة جواز السفر ، أو رخصة القيادة وتصعب الإجراءات أو تسهل تبعاً للغرض من إستخدامها[2].

- **صور الإعتداء على التوقيع الإليكترونى وفقاً لنصوص القانون رقم 15 لسنة 2004 فى مصر :**

نصت المادة 21 من هذا القانون بأن (بيانات التوقيع الإليكتروني والوسائط الإليكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإليكتروني سرية ، ولا يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها للغير أو إستخدامها في غير الغرض الذي قدمت من أجله).

وكذلك نصت مادة 23 بأنه مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر ، يعاقب بالحبس وبغرامة لاتقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من :

(أ) أصدر شهادة تصديق إليكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة.

(ب) أتلف أو عيّب توقيعا أو وسيطا أو محرراً إليكترونيا ، أو زوّر شيئا من ذلك بطريق الإصطناع أو التعديل أو التحوير أو بأي طريق آخر .

(ج) إستعمل توقيعا أو وسيطا أو محرراً إليكترونيا معيباً أو مزوراً مع علمه بذلك.

(د) خالف أيّا من أحكام المادتين (19) ، (21) من هذا القانون .

---

(1) محمد عبيد الكعبى ، ص 240 . 241.

(2) محمد عبيد الكعبى ، ص 242.

(هـ) توصّل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إليكتروني أو إخترق هذا الوسيط أو إعترضه أو عطله عن أداء وظيفته.

وفي حالة العود تزاد بمقدار المثل المقررة ، العقوبة المقررة لهذه الجرائم في حديها الأدنى والأقصى . وفي جميع الأحوال يحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الإنتشار ، وعلى شبكات المعلومات الالكترونية المفتوحة على نفقة المحكوم عليه.

وبناء على ما أجملنا فإن أبرز صور الإعتداء على التوقيع الإليكترونى هى:

1 ـ جريمة إفشاء بيانات التوقيع الإليكترونى أو إستخدامها فى غير الغرض المخصصة لأجله:

صورة الركن المادى فى هذه الجريمة هى إفشاء بيانات التوقيع الإليكترونى والوسائط الإليكترونية والمعلومات التى تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإليكترونى أو إستخدامها فى غرض آخر غير ما قدمت له[1].

والمقصود هنا بإفشاء البيانات ، هو تمكين الغير من الإطلاع عليها بشكل علنى ، أما الشق الثانى المنصوص عليه فى هذه الجريمة فهو إستخدام بيانات التوقيع الإليكترونى من قبل الجهة المرخص لها بإصداره فى غير الغرض المقدمة من أجله.

إضافة إلى الركن المادى يلزم توافر الركن المعنوى بعنصريه العلم والإرادة ، وذلك بأن يكون الجانى عالماً بعدم مشروعية فعله ، وإتجاه إرادته رغم ذلك لإرتكابه.

2 ـ إصدارشهادة تصديق إليكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة:

عرف القانون 15 لسنة 2004 فى المادة الأولى فقرة (و) شهادة التصديق الإليكترونى بأنها الشهادة التى تصدر من الجهة المرخص لها بالتصديق وتثبت الإرتباط بين الموقع وبيانات إنشاء التوقيع.

وبناء على ذلك توجد جهات يرخص لها سواء كانت شخصية أو إعتبارية بإعتماد التوقيعات الإليكترونية بشهادات مصدق عليها منهم ، وهذه الشهادات يترتب عليها آثاراً قانونية تتمثل فى إنشاء إلتزامات وإثبات حقوق بالنسبة لطرفى العقد فى التجارة الإليكترونية فى حالة إعتماد التوقيع الإليكترونى بينهما[2]، وبالتالى فإن قيام أى جهة بإصدار شهادات التصديق هذه دون الحصول على الترخيص اللازم لصحة إجراءها ، يعد ركناً مادياً لهذه الجريمة إضافة للركن

---

(1) د. سليمان أحمد فضل ، المرجع السابق ، ص161.

(2) د. حسين بن سعيد الغافرى ، الجرائم الواقعة على التجارة الإليكترونية ، المرجع السابق ذكره ، ص10.

المعنوى بعنصريه.

3 - إتلاف أو تعييب توقيعا أو وسيطا أو محرراً إليكترونياً ، أو تزوير شيئاً من ذلك بطريق الإصطناع أو التعديل أو التحوير أو بأي طريق آخر.

تنقسم هذه الجريمة إلى قسمين القسم الأول متعلق بجريمة الإتلاف أو التعييب للمحرر الإليكترونى ، والثانى متعلق بتزويره.

أ. إتلاف أو تعييب توقيع أو وسيط أو محررإليكترونى.

صورة الركن المادى لهذه الجريمة هى إتلاف أو تعييب للتوقيع أو المحرر أو الوسيط الإليكترونى ، وجريمة الإتلاف تقع طالما وقع ثمة إتلاف أو تخريب على المال على نحو يذهب بقيمته كلها أو بعضها ، ولا يتحتم أن يكون التخريب أو الإتلاف تاماً بل يصح أن يكون جزئياً ، ولا يهم الوسيلة المستخدمة فى تلك الجريمة، والعنصر الثانى فى الركن المادى هو المحل الذى يرد عليه هذا الفعل والمحل فى هذه الجريمة هو التوقيع الإليكترونى أو الوسيط أو المحرر الإليكترونى(1). إضافة إلى الركن المادى فى هذه الجريمة يلزم توافر الركن المعنوى بعنصريه العلم والإرادة.

ب . تزوير التوقيع الإليكترونى أو الوسيط أو المحرر الإليكترونى.

الركن المادى لهذه الجريمة يدور حول فعل التزوير أو التقليد الإليكترونى ، والذى يقصد به أى تغيير للحقيقة يرد على مخرجات الحاسب الآلى سواء تمثلت فى مخرجات ورقية مكتوبة كتلك التى تتم عن طريق الطابعة أو كانت مرسومة عن طريق الراسم ، ويستوى فى المحرر الإليكترونى أن يكون مدوناً باللغة العربية أو لغة أخرى لها دلالتها ، كذلك قد يتم فى مخرجات غير ورقية شرط أن تكون محفوظة على دعامة . كبرنامج منسوخ على إسطوانة. وشرط أن يكون المحرر الإليكترونى ذا أثر فى إثبات حق أو أثر قانونى معين(2).

ومن أشهر الوسائل التى يمكن الإعتماد عليها فى تقليد أو تزوير التوقيع الإليكترونى إستخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك ، يتم تصميمها على غرار البرامج والأنظمة المشروعة أو محاولة البعض كسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإليكترونى ، والقيام بنسخها وإعادة إستخدامها بعد ذلك ، وتعد هذه الجريمة من الجرائم العمدية ، التى تنطوى على قصد جنائى عام ، حيث يعلم الجانى بوقائع الجريمة وكونها من المحظورات

---

(1) د. سليمان أحمد فضل ، المرجع السابق ، ص 164.

(2) د.عبد الفتاح بيومى حجازى ، الدليل الجنائى والتزوير فى جرائم الكمبيوتر والإنترنت ، دار الكتب القانونية ، 2002 ، ص170.

، ومع ذلك تتجه إرادته إلى الفعل المجرم ويقبل النتيجة المترتبة عليها[1].

4 ـ إستعمال توقيعا أو وسيطا أو محرراً إليكترونيا معيباً أو مزوراً مع العلم بذلك.

يقصد بإستعمال التوقيع الإليكترونى المزور أو المعيب إبرازه والإحتجاج به فيما زور من أجله وذلك على إعتبار أنه صحيح[2].

وهذه الجريمة جريمة عمدية ، يلزم لقيامها أن يكون الجانى عالماً بعدم مشروعية فعله ، أى علمه بإستخدام توقيع أو محرر أو وسيط إليكترونى معيب أو مزور ، بغض النظر إن كان هو من زور أو عيب التوقيع أو لا.

5 ـ التوصّل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إليكتروني أو إختراق هذا الوسيط أو إعتراضه أو تعطيله عن أداء وظيفته.

يتمثل الركن المادى لهذه الجريمة فى حصول الجانى على توقيع إليكترونى بأى وسيلة غير مشروعة دون حق له فى ذلك، أو قيام الجانى بإختراق الوسيط الإليكترونى أو إعتراضه وتعطيله.

ومن الملاحظ فى هذه الجزئية عدم تحديد نص القانون لطرق أو وسائل معينة للحصول على التوقيع الإليكترونى أو إختراقه وتعطيله ، وهو مايوسع من مجال حماية التوقيع الإليكترونى ضد أى محاولة للإعتداء عليه.

أما الركن المعنوى فيتمثل فى إتجاه الجانى لإرتكاب الجريمة مقترناً بعلمه بعدم مشروعية فعله.

ثانياً : السطو على أرقام البطاقات الإئتمانية.

تعد بطاقات الإئتمان إحدى الخدمات المصرفية التى إستحدثها الفن المصرفى فى الولايات المتحدة الأمريكية منذ ما يقرب على 60 عام ، فأول بداية حقيقية لبطاقات الإئتمان بالمفهوم الحديث ترجع للأمريكيين (فرانك بيكن مارا ورالف سيندر) فى عام 1950م ، وتقوم هذه البطاقات أساساً على فكرة الإئتمان لإفتراضها وجود فاصل زمنى بين تقديم مانح الإئتمان لوسائل الوفاء لعملية الشراء وبين إسترداد تلك الوسائل ، وبعد التطور الكبير التكنولوجى فى مجال الإتصالات وظهور التجارة الإليكترونية ، إمتد نشاط هذه البطاقات إلى شبكة الإنترنت الذى شكل عملية متسارعة لكونه يعد إحدى الطرق السهلة لشراء كل شيء تقريباً ، فكل ما يحتاجه

---

(1) د. حسين بن سعيد الغافرى ، الجرائم الواقعة على التجارة الإليكترونية ، المرجع السابق ذكره ، ص10 . 11.

(2) د. سليمان أحمد فضل ، المرجع السابق ، ص 165.

التسوق عبر الإنترنت هو إتصال بالإنترنت وبطاقة إئتمان سارية المفعول[1].

وتعتمد آلية الشراء عبر شبكة الإنترنت بإستخدام البطاقات الإئتمانية على تزويد التاجر برقم البطاقة الخاصة بالعميل والعنوان الذى يرغب بإستلام السلعة من خلاله ومعلومات أخرى ، ليصله طلبه خلال الفترة الزمنية التى تم الإتفاق عليها ، فى الوقت الذى تتولى فيها شبكات البنوك العالمية والشركات إجراء عملية التقاص بين الحسابات وقيد الفوائد والعمولات وفقاً للإتفاقيات والبوتوكولات بهذه الشأن[2].

إلا أن هذه الميزة الإيجابية لعملية الشراء بإستخدام شبكة الإنترنت قابلها إستغلال غير مشروع لمواطن الضعف التى كشف عنها التطبيق الفعلى لهذه النظام ، حيث أصبحت الأرقام والبيانات الخاصة بتلك البطاقات المنقولة عبر شبكة الإنترنت عرضة للإلتقاط غير المشروع من قبل الغير وبالتالى الإعتداء على الذمة المالية لصاحب البطاقة أو البنك المصدر لهذه البطاقة.

ففى اليابان ألقت الشرطة القبض على رجلين قاما بسرقة 16 مليون ين من حساب عميل أحد البنوك ، بعد تمكنهما من سرقة بيانات بطاقته الإئتمانية من خلال ترددهما على مقاهى الإنترنت[3]، وفي مصر تكلف جرائم التجارة الإليكترونية الدولة حوالي3 ملايين جنيه سنويا تتحملها البنوك المصرية[4].

- **طرق السطو على أرقام البطاقات الإئتمانية:**

1. الإستدراج أو الصيد phishing:

أخذت هذه التسمية من كلمة Fishing والتى تعنى صيد السمك، ويعتبر من أحدث الأساليب المستخدمة فى جرائم الهاكرز عالمياً ونسبة نجاحه 5%[5].

ويعد من قبيل الإستدراج إنشاء مواقع وهمية على شبكة الإنترنت على غرار مواقع

---

(1) د. حسين بن سعيد الغافرى ، الجرائم الواقعة على التجارة الإليكترونية ، المرجع السابق ذكره ، ص22.

(2) عماد على الخليل ، التكييف القانونى لإساءة إستخدام أرقام البطاقات الإئتمانية عبر الإنترنت ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد بكلية الشريعة والقانون بجامعة الإمارات العربية المتحدة فى الفترة من 1: 2000/5/3 ، المجلد الثانى ص909 ، مشار إليه لدى د .حسين بن سعيد الغافرى ، المرجع السابق ، ص23.

(3) www.albayan.co.ae/albayan/mnw/15.htm

(4) تحقيق بعنوان مواجهة حاسمة من الشرطة لجرائم بطاقات الائتمان الإلكترونية ، جريدة الأهرام ، بتاريخ 2002/5/18، السنة 126 ، العدد 42166 ، راجع الموقع الإليكترونى
http://www.ahram.org.eg/Archive/2002/5/18/ECON5.HTM

(5) د. حسين بن سعيد الغافرى ، الجرائم الواقعة على التجارة الإليكترونية ، المرجع السابق ذكره ، ص23.

الشركات والمؤسسات التجارية الأصلية التى توجد على الشبكة ، ويظهر وكأنه هو الموقع الأصلى الذى يقدم الخدمة ، ولإنشاء هذا الموقع يقوم القراصنة بالحصول على كافة بيانات الموقع الأصلى من خلال شبكة الإنترنت ، ومن ثم إنشاء الموقع الوهمى ومع تعديل البيانات السابقة التى تم الحصول عليها بطريق غير مشروع . وذلك فى الموقع الأصلى . حتى لا يظهر وجود إزدواج فى الموقع ويبدو الموقع الاصلى وكأنه الموقع الوحيد[1].

ويتحقق الضرر بإستقبال الموقع الوهمى الخاص بالقراصنة على شبكة الإنترنت لكافة المعاملات المالية والتجارية الخاصة بالتجارة الإليكترونية ، والتى يقدمها الموقع الأصلى عبر الشبكة لأغراض هذه التجارة ، ومنها بالطبع بيانات بطاقة الدفع الإليكترونى ، وكذلك الرسائل الإليكترونية الخاصة بالموقع الأصلى ومن ثم يتسنى الإطلاع عليها والإستفادة غير المشروعة من المعلومات المتضمنة فيها ، وذلك على نحو يضر بالمؤسسات والشركات صاحبة الموقع الاصلى ، وفى ذات الوقت يدمر ثقة الافراد والشركات فى التجارة الإليكترونية عبر شبكة إنترنت[2].

ومن أشهر الأمثلة على إستخدام هذه الأسلوب فى الحصول على أرقام وبيانات البطاقات الإئتمانية المنقولة على شبكة الإنترنت ، ما حصل عام 1994 عندما قام شخصان بإنشاء موقع على شبكة الإنترنت مخصص لشراء حاجات معينة يتم إرسالها فور تسديد قيمتها إليكترونيا ، إلا أن الطلبات فى حقيقة الواقع كانت لا تصل إلى الزبائن لأن الموقع ببساطة ما هو إلا موقع وهمى هدفه النصب والإحتيال.

وفى مصر كذلك ألقت السلطات المصرية القبض على 43 شخصاً قاموا بتزوير الصفحات الرئيسية للمواقع الإليكترونية لبنكى أوف أمريكا ويلز فاركو بأمريكا، وقاموا بإرسال عدة رسائل إليكترونية لبعض عملاء هذين البنكين . وكأنها عبر المواقع الإلكترونية الصحيحة للبنكين . وقاموا بطلب تحديث بياناتهم البنكية، وإستخدموا البيانات وأجروا عدة حجوزات فندقية، وشراء تذاكر طيران، وتحويلات مالية بقيمة مليون و117 ألف دولار أمريكى لحسابات أخرى بذات البنكين[3].

---

(1) راجع فى ذلك د. جميل عبد الباقى الصغير ، الحماية الجنائية والمدنية لبطاقات الإئتمان الممغنطة ، دار النهضة العربية ، 1999 ، ص 37.

(2) الرائد.على حسنى عباس، مخاطر بطاقات الدفع الإليكترونى عبر شبكة الإنترنت (المشاكل والحلول) ، ورقة عمل مقدمة إلى ندوة (الصور المستحدثة لجرائم بطاقات الدفع الإليكترونى) مركز بحوث الشرطة بأكاديمية الشرطة ، القاهرة ، بتاريخ 1998/12/14. ص17.

(3) راجع الموقع : http://www.egypty.com/accidents-details.aspx?accidents=3030

2 . الإختراق غير المشروع لمنظومة خطوط الإتصالات العالمية Illegal access :

خطوط الإتصالات العالمية هى تلك الخطوط التى تربط الحاسب الآلى للمشترى بذلك الخاص بالتاجر، ويعد الإختراق غيرالمشروع لمنظومة خطوط الإتصالات العالمية من أخطر الأساليب التى تهدد عملية التسوق عبر شبكة الإنترنت ، حيث يقوم المقتحم بتسخير كل خبراته وبرامجه لمحاولة إقتحام وفك رموز الشفرات وتجاوز جدر الحماية للملفات المتضمنة للمعلومات الشخصية للعملاء والمخزنة فى الكمبيوتر الرئيسى عبر الشبكة العنكبوتية ، والدافع الأساسى من اللجوء إليه يتمثل فى الرغبة الكامنة فى نفوس محترفى الإجرام التقنى فى قهر نظم التقنية والتفوق على الحماية وتعقيدها(1).

3 . تقنية تفجير الموقع المستهدف:

تمتلك كبرى الشركات والمؤسسات فى مختلف دول العالم مواقع إليكترونية على شبكة الإنترنت ، هذه المواقع يتم إدارتها من قبل أجهزة كمبيوتر خاصة بالشركة أو المؤسسة ، ولكن يوجد دائماً جهاز رئيسى أومايعتبر الجهازالأم لهذه الأجهزة الفرعية ، وهو الذى يتم من خلاله تعديل الموقع وإضافة البيانات المستحدثة ، وكذلك يحتوى كافة البيانات المتعلقة بطبيعة العمل المقدم من الشركة أو المؤسسة والتى قد يكون من بينها أرقام بطاقات إئتمان خاصة بالعملاء، ويتم الحصول على أرقام بطاقات الإئتمان من خلال هذا الجهاز عن طريق قيام المحتال بإرسال الآلاف من الرسائل الإليكترونية لهذا الجهاز بهدف الضغط على قدرته الإستيعابية وبالتالى تفجير الموقع الذى يقوم الجهاز بخدمته ، الأمر الذى يترتب عليه إنتقال كل البيانات التى يحتويها هذا الجهاز إلى شخص المجرم.

4 . تخليق أرقام البطاقات الإئتمانية:

يعرف هذا الأسلوب لدى مجرمى البطاقات بـ (Card Math) وهو يعتمد بالدرجة الأولى على إجراء معادلات رياضية وإحصائية بهدف تحصيل أو تخليق أرقام بطاقات إئتمانية مملوكة للغير ، وهى ما يلزم للشراء عبر شبكة الإنترنت(2)، ومن الأمثلة على إستخدام هذا الأسلوب ما حصل بجمهورية مصر العربية حيث تمكنت الإدارة العامة لمباحث الأموال العامة من ضبط طالب جامعى بمدينة الإسكندرية بتهمة الإستيلاء على مبالغ طائلة من حسابات بعض البطاقات الإئتمانية الخاصة بعملاء أحد البنوك بالجيزة عبر شبكة الإنترنت وإستخدامها فى عمليات الشراء والتسوق ، بعدما تمكن من الحصول على أرقام تلك البطاقات بإستخدام بعض المعادلات

---

(1) د. حسين بن سعيد الغافرى ، المرجع السابق ، ص23.

(2) عماد على الخليل ، المرجع السابق ، ص5.

الحسابية الدقيقة.

وللحد من هذه الجرائم قام البعض من العلماء بإختراع بطاقات إئتمان جديدة مختلفة عن سابقاتها ، تعمل ببصمة صوت صاحبها فقط ليس ذلك وحسب بل أن هذه البصمة الصوتية تتغيربعد كل مرة يتم فيها إستخدام البطاقة.

ومن وسائل الحد من هذه الجرائم أيضاً ما قام به بنك (سيتى بنك) وهى الطريقة أو الوسيلة المعروفة بإسم الحساب المؤقت ، حيث يسمح لعملائه بفتح حساب مؤقت للشراء عبر شبكة الإنترنت يمكن الحصول عليه بالتليفون أو البريد ، ويستخدم لمرة واحدة فقط ثم يلغى بعد ذلك ، أو لأكثر من مرة بحيث يصل إلى سقف إئتمانى محدد ، وهو مرتبط بالحساب الأساسى للعميل(1)، وفوق كل ذلك لابد من تثقيف الجمهور عن طبيعة المخاطر الأمنية التي تواجهها وكيف يمكن حماية أنفسهم من خلال إتخاذ الإحتياطات الأمنية الأساسية[2].

ويتحقق الركن المادى فى جريمة السطو على أرقام بطاقات الإئتمان بإتيان الأفعال الإجرامية السابق ذكرها (الإستدراج ، الإختراق غير المشروع ، تفجير الموقع ، تخليق أرقام البطاقات) إضافة للنتيجة المترتبة على هذا الفعل مع وجود علاقة سببية بين الفعل والنتيجة.

أما الركن المعنوى فيجب توافر عنصريه (العلم والإرادة) وذلك بأن يكون الجانى عالماً بأنه يستولى على أرقام بطاقة إئتمانية تخص المجنى عليه ورغم ذلك يقدم على هذا الفعل.

ثالثاً : الإعتداء على حقول الإنترنت:

يشير مصطلح حقل الإنترنت أو كما يعرف بالإنجليزية (Domain) إلى موقع إليكترونى معين، فكل موقع على شبكة الإنترنت لابد وأن يحمل إسماً أو عنواناً معيناً يميزه عن غيره من المواقع الإليكترونية، وهو ما يعرف بالحقل فحقل الإنترنت هو عنوان موقع إليكترونى ما.

فمثلاً موقع جوجل يشار إلى حقله بإسم www.google.com ، ولكل متصفح يريد الولوج لهذا الموقع أن يكتب هذا الإسم.

ويمكن تعريف حقول الإنترنت أو مواقع الإنترنت بأنها مجموعة من الوثائق الموضوعة

(1) http://www.al-jazirah.com.sa/digimag/20062004/wr25.htm

(2) Russell G. Smith , paying the price on the internet, funds transfer crime in cyberspace, paper presented at the conference: internet crime, held in melbourne, 16-17 february 1998, by the australian Institute of Criminology, p8.

إليكترونياً فى حاسبات مختلفة متصلة بالإنترنت(1).

ويمكن تعريف حقل الإنترنت كذلك بأنه إسم فريد يُعرِّف موقع واحد على شبكة الإنترنت، و هو مؤلف من قسمين أو أكثر و يفصل بين أقسامه بالنقطة{.}(2).

مع الأخذ بالعلم أن الدومين أو الحقل لا يمكن أن يكون مكتوب باللغة العربية بل يجب حجزه باللغة الانجليزية.

والأصل فى مواقع الإنترنت أنه ينبغى للوصول إليها معرفة عناوينها التى هى عبارة عن أرقام معينة ، ونظراً لكثرة المواقع وبالتالى تعذر حفظ أرقام كل موقع بالنسبة لمستخدمى الشبكة ، تم إبتكار ما يعرف بالدومين نيم Domain Name ، وهو ما سهل الإشارة لأسماء المواقع وسهولة التمييز فيما بينها.

فالدومين نيم هو نقل إسم الموقع من صيغة إلى أخرى أو بمعنى أصح نقله من صيغته الرقمية إلى الصيغة أو الصورة الحرفية.

ويشكل إسم حقل الإنترنت من الناحية الإقتصادية وسيلة فعالة للإعلان عن المشروعات والشركات والتعريف بها وعرض منتجاتها وخدماتها(3)، فالشركات التجارية تستخدم مواقعها الإليكترونية فى عرض البيانات الخاصة بالشركة كطبيعة نشاطها وأرقام هواتفها وعنوان بريدها العادى والإليكترونى.

- **أشكال أسماء حقول الإنترنت:**

يتكون إسم الحقل من عدة أجزاء ، عادة ما يكون الجزء الأول من اليسار وهو المعروف بـ www وهو إختصار لمصطلح World Wide Web أو الشبكة العالمية الواسعة ، أما الجزء الثانى من إسم الحقل فهو إسم أو رمز أو إختصار المؤسسة أو الشخص أو الجهة مالكة الموقع مثل Aljazeera أو Alarabiya أما الجزء الأخير من العنوان فقد يكون على عدة أشكال مثل:

- (com) تدل على الشركات التجارية.
- (edu) تدل على مؤسسات التعليم.

---

(1) حسين سعيد الغافرى ، المرجع السابق ، ص 12.

(2) البوابة العربية للكمبيوترعلى الإنترنت راجع الموقع،
http://www.fursansouria.org/acg/domain_name_definition.html

(3) مهندس/رأفت رضوان ، إتجاهات مجتمع الأعمال العربى نحو التجارة الإليكترونية ، بدون دار نشر ، 1999 ، ص245.

- (gov) تدل على المواقع الحكومية.
- (mil) للجيش والهيئات العسكرية.
- (org) للمنظمات.
- (Info) تدل على مواقع المعلومات.

- **أشكال الإعتداء على حقول الإنترنت:**

تتعدد أشكال الإعتداء على المواقع الإليكترونية وغالباً ما يهدف الجانى فى جرائم الإعتداء على حقول وأسماء الإنترنت إلى الحصول على منفعة معينة من وراء ذلك ، وإذا لم يتسنى له ذلك فإنه على أقل تقدير يلحق الضرر بالموقع الإليكترونى المستهدف ، مع ملاحظة أن ثمة جرائم تقع ضد الموقع الإليكترونى ذاته تؤدى إلى إلحاق أضرار مادية به أو تفويت ربح متوقع بأى شكل كان، أو جرائم أخرى تقتصر على الإستيلاء على إسم موقع تجارى أو محاكاته بهدف التغرير بزبائن هذا الموقع وتحصيل مكاسب مالية.

وفيما يلى إجمال لأبرز الطرق التى يتم فيها الإعتداء على مواقع الإنترنت:

أ . **تدمير المواقع** : يستطيع بعض محترفى جرائم الإنترنت تدمير أيا من مواقع الإنترنت ، وذلك بعدة وسائل كبرامج معدة لذلك ، أو بطرق أخرى تقوم على إستغلال الثغرات الموجودة فى هذه المواقع تتمثل فى عدم وجود تأمين كافى فى مواجهة الإختراقات والقيام بتدمير قواعد البيانات فيها ، الأمر الذى يؤدى إلى شل كامل أو جزئي في عمل الموقع مما قد يكبد الشركات والمؤسسات والأفراد خسائر مادية ومعنوية.

ومن أبرز الامثلة على تدمير المواقع تعرض موقع Hotmail فى العام 2000 لبعض الهجمات أدت لخسائر مالية تعدت ملايين الدولارات[1].

ب. **تشويه صورة المواقع التجارية:** صورة أخرى من صور الإضرار بمواقع التجارة الإليكترونية ، لا لشىء إلا لإثبات الذات وإبراز ضعف الموقع المستهدف وفى نفس الوقت الإضرار والتشويه بسمعة الموقع فى مواجهة زائريه ورواده.

ويتم تشويه صورة المواقع على شبكة الإنترنت عن طريق دخولها بهوية مخفية(anonymous) حيث تمكن هذه الطريقة، في بعض الحالات، المخترق من الحصول على ملف كلمة الدخول المشفرة، الخاصة بأحد المشرفين على الموقع المستهدف، أو من يملكون حق تعديل محتويات الموقع، والعمل على فك تشفيرها،

(1) www.khayma.com/tanweer/textes/hacar.htm

ويستعين المخترقون فى ذلك ببرامج خاصة لتخمين كلمات السر [1].

ج . **هجمات حجب خدمة الإنترنت:** "الوصول إلى هذا الموقع غير ممكن" قد تعني الرسالة السابقة أن الموقع الذي تحاول أن تزوره، تعرض لهجمات حجب الخدمة خاصة إذا كان واحداً من المواقع الكبرى التي يعني ظهور مثل هذه الرسالة في موقعها خسارة عشرات الآلاف من الدولارات [2].

د . **إختلاس مضمون مواقع الإنترنت:** يعمد البعض إلى نسخ محتويات بعض المواقع الإليكترونية وإعادة نشرها فى أى موقع آخر دون الإشارة لمصدرها ، بغض النظر عن مضمون هذه المحتويات فقد تكون صور أو نصوص أو رسومات أو مقاطع فيديو ، الأمر الذى يثير الكثير من الإشكالات والقضايا بين المواقع نظراً للخسائر المادية والأدبية التى تلحق بالطرف المعتدى على حقه[3].

هـ . **إنتحال شخصية الموقع:** المقصود بإنتحال شخصية الموقع هو إنتحال صفة مؤسسة أو جهة تملك موقعاً على شبكة الإنترنت ، و لعل الطابع الشائع منها هو إنتحال صفة مواقع تتعامل عن طريق الدفع الإليكتروني للأموال والغرض هنا هو الوصول إلي بيانات بطاقات الدفع التي يتعامل بها الأشخاص الذين يدخلون للمواقع أو كشف بيانات الحسابات البنكية ثم الدخول لها وإجراء عمليات غير شرعية بها أو إجراء تحويلات من هذه الحسابات إلى حسابات أخرى.

الفرع الثالث

جرائم التجارة الإليكترونية فى المنظور التشريعى

التجارة الإليكترونية وبما أنها نوع مستحدث من التجارة خصوصاً فى مجتمعاتنا العربية ، فإنها لا تزال تحتاج الكثير من التنظيم التشريعى الذى يغطى كافة المسائل المتعلقة بها.

ففى مصر نجد أن المشرع قد أقر قانون تنظيم التوقيع الإليكترونى رقم 15 لسنة 2004 والذى كفل التوقيع الإليكترونى بحماية فى مواجهة بعض صور الإنتهاكات الواقعة عليه وذلك

---

(1) فادي سالم ، مقال بعنوان موقعك في ويب.. في مهب الإختراق ، صحيفة الحوار المتمدن الإليكترونية ، العدد رقم: 15 بتاريخ 23/ 12 / 2001 . راجع الموقع
http://www.ahewar.org/debat/show.art.asp?aid=550

(2) فادي سالم ، المرجع السابق.

(3) راجع فى نفس المعنى ، د. محمد حسين منصور ، المسئولية الإليكترونية ، دار الجامعة الجديدة ، 2003 ، ص 259.

فى المادتين 21 ، 23 سابقتى الذكر.

إضافة لذلك فإن مشروع قانون التجارة الإليكترونية قد نص فى المادة 27 منه على أنه "مع عدم الإخلال بأية عقوبة أشد وردت فى قانون آخر ، يعاقب كل من إستخدم توقيعا إلكترونيا أو محا أو عدل فى هذا التوقيع أو فى مادة المحرر دون موافقة كتابية مسبقة من صاحب الحق بالغرامة التى لا تقل عن ألف جنيه ولا تزيد على ألفى جنيه ، وبالحبس الذي لا يقل عن ثلاثة أشهر أو بإحدى هاتين العقوبتين.

وفى حالة العود تكون العقوبة الغرامة التى لا تقل عن ألفى جنيه ولا تزيد على خمسة آلاف جنيه ، والحبس لمدة لا تقل عن ثلاثة أشهر. وفى كل الأحوال تحكم المحكمة بعدم الإعتداد بالمعاملة. "

وكذلك نص فى المادة 16 على أنه " لا يجوز لأية جهة تحصل على بيانات شخصية أو مصرفية خاصة بأحد العملاء أن تحتفظ بها إلا للمدة التى تقتضيها طبيعة المعاملة ، وليس لها أن تتعامل فى هذه البيانات بمقابل أو بدون مقابل مع أية جهة أخرى بغير موافقة كتابية مسبقة من صاحبها"

هذا النص يتعلق بالحفاظ على سرية البيانات وتجريم الإعتداء على الحق فى الخصوصية فى شأن البيانات الشخصية أو المصرفية التى يتمكن أحد المتعاقدين من الحصول عليها بصدد المعاملات التجارية الإلكترونية والتى قد يكون من بينها توقيعاً إليكترونياً.

أما بالنسبة لجرائم السطو على أرقام بطاقات الإئتمان فلم تسن نصوصاً خاصة بها ، الأمر الذى نظن معه بصحة إنطباق نصوص قانون العقوبات التقليدية المتعلقة بالسرقة أو النصب والإحتيال.

وإذا تطرقنا لجرائم الإعتداء على حقول وأسماء الإنترنت فلم تكن هى الأخرى أوفر حظاً من جرائم السطو على أرقام بطاقات الإئتمان وبقيت دون نظام تشريعى يفرد أركانها ويبين أصنافها وعقوباتها مما يجعل . ووفقاً لما نظنه صحيحاً . نصوص قانون العقوبات هى الأولى بالتطبيق وبشكل أدق النصوص المتعلقة بجرائم الإتلاف ، إضافةً إلى الحماية المقررة فى قوانين الملكية الفكرية.

أما فى تونس فقد نص قانون التجارة والمبادلات الإليكترونية فى إطار حمايته للتوقيع الإليكترونى على أنه يعاقب كل من إستعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بإمضاء غيره بالسجن لمدة تتراوح بين 6 أشهر وعامين وبخطية(غرامة) تتراوح بين 1.000 و 10.000 دينار أو بإحدى هاتين العقوبتين.

أما نظام الجرائم المعلوماتية في السعودية فقد نص فيما يخص الإعتداء على حقول الإنترنت فى المادة الثالثة منه على أنه: "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

1. ....

2. ....

3. الدخول غير المشروع إلى موقع إليكتروني، أو الدخول إلى موقع إليكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

وفى سبيل حماية التوقيع الإليكترونى وبطاقات الإئتمان نصت المادة الرابعة من النظام على : يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين ، كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

1. الإستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الإحتيال، أو إتخاذ إسم كاذب، أو إنتحال صفة غير صحيحة .

2. الوصول – دون مسوغ نظام صحيح – إلى بيانات بنكية أو إئتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

أما على المستوى الدولى فهناك قانون الأونسيترال النموذجى بشأن التوقيعات الإليكترونية ، وكذلك قانون الأونيسترال للتجارة الإليكترونية اللذان يطبقان على أى نشاط تجارى يتم عن طريق الوسائط الإليكترونية.

وكذلك التوصيات التى قدمتها المنظمة العالمية للملكية الفكرية المعروفة إختصاراً بإسم (ويبو) فيما يخص الإعتداء على أسماء حقول الإنترنت بوضع إجراء موحد لتسوية النزاعات المتعلقة بهذا الخصوص.

أما إتفاقية بودابست فقد جرمت الجرائم الواقعة على التجارة الإليكترونية ، فى المادة 8 ، حيث نصت على ضرورة إتخاذ كل دولة طرف فى الإتفاقية التدابير اللازمة فى مواجهة أى تدخل فى وظيفة منظومة كمبيوتر بقصد إحتيالى أو غير أمين للحصول على منفعة إقتصادية دون وجه حق لصالح المعتدى ذاته أو لصالح الغير وقد نصت الاتفاقية فى المادة 10 على ضرورة إتخاذ كل دولة طرف فى الإتفاقية التدابير اللازمة لحماية النواحى التجارية لحقوق الملكية الفكرية وكذلك الجرائم التى ترتكب عن طريق الكمبيوتر والتى تستهدف النطاق التجارى.

المطلــب الثانــى
جرائــم الإتــلاف المعلوماتى

الإتلاف هو تخريب الشىء موضوع الجريمة ، وذلك بجعله غير صالح للإستعمال أو الإنتفاع به ، أو كذلك التقليل من منفعته.

وبمعنى آخر فإن الإتلاف لا يخرج عن كونه فناء للشىء أو جعله بحالة غير الحالة التى هو عليها بحيث لا يمكن الإستفادة منه وفقاً للغرض الذى وجد من أجله ، مما يعنى أن جوهر الإتلاف هو إفقار المال المتلف منفعته أو صلاحيته للإستعمال فى الغرض الذى وجد من أجله. أو هو التأثير على مادة الشىء على نحو يذهب أو يقلل من قيمته الإقتصادية عن طريق الإنتقاص من كفائته لأوجه الإستعمال المعد لها[1].

أما المعلوماتية التى هى محل الإعتداء فى جريمة الإتلاف ، فتعرف بأنها ذلك الإطار الذي يحوي تكنولوجيا المعلومات ، وعلوم الكمبيوتر ، ونظم المعلومات وشبكات الإتصال وتطبيقاتها في مختلف مجالات العمل الإنساني المنظم[2].

والمقصود ببرامج الحاسب الآلى التعليمات المثبتة على دعامة والتى يمكن قراءتها لأداء واجب معين عن طريق نظام معالجة هذه المعلومات وقراءتها بواسطة الحاسب الآلي، فالحاسب لوحده لا يمكن أن يؤدي الغرض المرجو منه، ولا بد من وجود برامج تحركه[3].

والإتلاف في المجال المعلوماتي قد يكون إتلاف مادي يقع على المكونات المادية المتصلة بالحاسب الآلي وملحقاته كالشاشة أو لوحة المفاتيح ، وقد يقع الإتلاف على المكونات المعنوية كالمعلومات والبيانات والبرامج على اختلاف أنواعها ووظائفها وهو ما سنتناوله بالبحث.

---

(1) د. محمود مصطفى ، شرح قانون العقوبات القسم الخاص ، الطبعة الثامنة ، دار النهضة العربية ، 1984 ، ص645.

(2) د. صبرى الحاج المبارك ، مقال بعنوان المعلومات ودورها فى التنمية ، راجع الموقع
http://informatics.gov.sa/details.php?id=295

(3) وجدي عبد الفتاح سواحل ، مقال بعنوان فيروسات الكمبيوتر الكابوس الدائم ،منشور على الموقع الإليكتروني www.islamonline.net/serviet/satellite?c=articleA

الفرع الأول
جريمة الإتلاف فى قانون العقوبات

نص قانون العقوبات المصرى على جريمة الإتلاف فى المادة 361 بنصه كل من خرب أو أتلف عمداً أموالاً ثابتة أو منقولة لا يمتلكها أو جعلها غير صالحة للإستعمال أو عطلها بأية طريقة يعاقب بالحبس مدة لا تزيد على ستة أشهر وبغرامة لا تجاوز ثلاثمائة جنيه أو بإحدى هاتين العقوبتين.

فإذا ترتب على الفعل ضرر مالى قيمته خمسون جنيهاً أو أكثر كانت العقوبة الحبس مدة لا تجاوز سنتين وغرامة لا تجاوز خمسمائة جنيه أو إحدى هاتين العقوبتين.

وتكون العقوبة السجن مدة لا تزيد على خمس سنين وغرامة لا تقل عن مائة جنيه ولا تجاوز ألف جنيه إذا نشأ عن الفعل تعطيل أو توقيف أعمال مصلحة ذات منفعة عامة أو ترتب عليه جعل حياة الناس أو صحتهم أو أمنهم فى خطر.

وكذلك نصت المادة 457 من قانون العقوبات الليبى كل من أتلف أو بعثر أو أفسد مالاً منقولاً أو غير منقول أو صيره غير نافع كلياً أو جزئياً يعاقب بالحبس مدة لا تجاوز سنة أو بغرامة لا تزيد على مائة جنيه وتقام الدعوى بناء على شكوى الطرف المتضرر.

- **الركن المادى لجريمة الإتلاف:**

يقوم الركن المادى لجريمة الإتلاف على إرتكاب فعل الإتلاف أو التخريب الذى بدوره يؤدى إلى هلاك الشىء أو إفناؤه أو التقليل من قيمته الإقتصادية ، أما الشق الثانى للركن المادى هو أن يكون محل الجريمة مال ثابت أو منقول ويشترط فى هذا المال أن يكون مملوكاً للغير، فإذا كان مملوكاً للجانى نفسه أو غير مملوك لأحد إنعدمت الجريمة.

- **الركن المعنوى:**

كأى جريمة عمدية يشترط فى جريمة الإتلاف توافر القصد الجنائى العام بعنصريه العلم والإرادة ، فيشترط سبق علم الجانى بإتلافه مال الغير وإتجاه إرادته لذلك، أما إذا لم يعلم بذلك سواء إعتقد بملكيته الشخصية لهذا المال أو إنعدام ملكيته للغير إنعدم القصد الجنائى.

وفى ذلك قضت محكمة النقض " من المقرر أن جريمة الإتلاف المؤثمة قانونا بنص المادة 361 من قانون العقوبات إنما هي جريمة عمدية يتحقق القصد الجنائي فيها متى تعمد الجاني ارتكاب الفعل المنهي عنه بالصورة التي حددها القانون واتجاه إرادته إلى إحداث الإتلاف

أو التخريب وعلمه بأنه يحدثه بغير حق ....." [1]

الفرع الثانى

المقصود بإتلاف معلومات وبرامج الحاسب الآلى

يقصد بإتلاف برامج الحاسب الآلى ومعلوماته إتلاف أو محو تعليمات البرامج أو البيانات ذاتها ويطلق عليه مصطلح تدمير نظم المعلومات ، وعادة لا يستهدف مرتكب هذه الإعتداء فائدة مالية لنفسه ، بل يسعى للإعاقة وتعطيل نظم المعلومات عن أداء وظائفها وإحداث أضرار بها[2].

وبهذا يتحقق الإتلاف المنصوص عليه فى المادة 361 من قانون العقوبات المصرى وكذلك المادة 457 عقوبات الليبى ، حيث أن جوهر الفعل المرتكب هو الإفساد أو التخريب وهو ما نصت عليه المادتين سالفتى الذكر.

وقد إستخدم المشرع فى ولاية كاليفورنيا بالولايات المتحدة الأميركية عدة تعبيرات للإشارة على مدلول الإتلاف ، مثل (عدل ، أفسد ، محى ، دمر) وهى تعبيرات تصب كلها فى نفس المعنى[3].

ويتمثل الركن المادى فى جريمة الإتلاف المعلوماتى بإحداث ضرر فى مال الغير وفى الحاسب الآلى تحديداً ، ويجب أن نفرق بين إتلاف جهاز الحاسب الآلى بحد ذاته كتكسير شاشته أو أحد ملحقاته الخارجية وهو ما ينبغى معه . وفقاً للمنطق . تطبيق نصوص قانون العقوبات المتعلقة بالإتلاف دون شك ، وبين الحالة التى يمتد فيها الإتلاف إلى برامج ونظم الحاسب الآلى نفسه أى ما يحويه من معلومات ومعطيات ، وهو الأمر الذى لم تشمله نصوص قانون العقوبات المتعلقة بالإتلاف.

ويتحقق الركن المادى لجريمة الإتلاف المعلوماتى بإرتكاب إما فعل الإتلاف أو التخريب أو التعطيل أو بجعله غير صالح للإستعمال ، ويقصد بالإتلاف إفناء الشىء أو هلاكه كلياً ، ويقصد بالتخريب توقف الشىء تماماً عن أداء منفعته حتى مع عدم فناء مادته سواء كان هذا

---

(1) الطعن رقم 19622 لسنة 62 ق جلسة 6/7/1997 س 48 ص 740.

(2) Walter Gary Sharp, Redefining National Security in Today's World of information technology and Emergent Threats, 9 Doke J Comp and Int'l p 383-384 (1999).

(3) Eric J. Sinrod, and William P Reilly, "Cyber-Crimes: A practical approach to the Application of Federal Computer Crimes Laws, 16 Santa Clara computer and High Tech L.J 177, p 90, (2000).

التوقف كلياً أو جزئياً ، ويكون الشيء غير صالح للإستعمال بجعله لا يؤدى وظيفته على النحو المطلوب أما التعطيل فيكون بتوقف الشيء عن القيام بوظيفته لفترة مؤقته ، وتتحقق جريمة الإتلاف بتحقق إحدى هذه النتائج[1].

والعبرة فى إتلاف الشيء هو إنقاص قيمته ولذلك فإن محل الحماية الحقيقى هو قيمة الشيء وليس حماية مادته إلا وسيلة لحماية قيمته ، فإذا كان الفعل قد افقد الشيء قيمته إذا نقص منها فقد حقق الإعتداء الذى يعاقب عليه القانون بإعتباره قد ذهب بأهمية الشيء بالنسبة إلى مالكه[2].

- **محل جريمة الإتلاف المعلوماتى:**

الإتلاف المعلوماتى لا يكون محله إلا برامج وبيانات الحاسب الآلى ، وذلك بغرض تدميرها أو محوها كلها أو بعضها لغرض الإنتقام أو المنافسة أوماشابه ذلك ، وعلى العكس من الإتلاف الواقع على جهاز الكمبيوتر ذاته أو على أحد ملحقاته الذى يستوجب منطقياً تطبيق نصوص قانون العقوبات ، فإن الأمر يختلف بالنسبة للبرامج والبيانات والمعطيات نظرا للقيمة المعنوية غير المادية لهذه البرامج ، وهو ما أثار تساؤلاً فقهياً عن مدى إمكانية تطبيق قانون العقوبات التقليدى من عدمه ، وإنقسم الفقه فى ذلك إلى إتجاهين أحدهما مؤيد لفكرة تطبيق قانون العقوبات على جرائم الإتلاف المعلوماتى ، والآخر رافض لهذه الفكرة ، وفيما يلى عرض لكل إتجاه.

الإتجاه الأول:

يرى أنصار هذا الرأى عدم إمكانية تطبيق قانون العقوبات على هذه الجريمة وحججهم فى ذلك هى:

1. أن القانون أو النظام لا يحمى فى الأصل إلا مادة الشيء وذلك توصلاً إلى توفير الحماية القانونية لقيمته الإقتصادية التى تعتمد على بقاء مادته صالحة وفقاً للغرض منها[3].
2. لا تعد البيانات والبرامج مالاً فى حد ذاتها وبالتالى لا يمكن أن يتم تملكها ، حيث أن حق الملكية لا ينصب إلا على الأشياء المادية التى لها قيمة إقتصادية وقيمة مادية وهو ما لا ينطبق على جرائم الحاسب الآلى.

---

(1) د. عفيفى كامل عفيفى ، مرجع سابق ، ص 183.

(2) د. جميل عبد الباقى الصغير ، القانون الجنائى والتكنولوجيا الحديثة ، الكتاب الأول ، الجرائم الناشئة عن إستخدام الحاسب الآلى ، دار النهضة العربية ، 1992 ، ص127.

(3) د. جميل عبد الباقى الصغير ، المرجع السابق ، ص159.

الإتجاه الثانى:

يرى أنصار هذا الإتجاه ضرورة تطبيق نصوص قانون العقوبات على الجريمة ويستندون للحجج الآتية:

1. أن المادتين 361 من قانون العقوبات المصرى و 457 عقوبات ليبى ، قد نصتا على أن الإتلاف يقع على الأموال المنقولة ولم تشترطا أن يكون المال محل الإعتداء مالاً مادياً ملموس بل جاء اللفظ عاماً دون تقييد ، مما يعنى جواز تطبيق نصوص قانون العقوبات على الجريمة.

2 . أن برامج الحاسب الآلى تنتج من قبل شركات متخصصة فى هذا المجال وتقدمها بمقابل ، ونعنى بذلك أن برامج الحاسب الآلى ذات قيمة إقتصادية ومالية تستوجب الحماية القانونية لملكية أصحاب هذه البرامج.

3. عدم وجود نصوص خاصة بهذه الجريمة فى قانون العقوبات أو غيره من القوانين ، وبالتالى أولوية تطبيق قانون العقوبات ولوقياساً.

وبعد العرض لكل من الإتجاهين ، فإنه ووفقاً للمنطق فإن الإتجاه الثانى القاضى بتطبيق نصوص قانون العقوبات هو الأولى والأجدر بالتأييد ، وإعتبار برامج الحاسب الآلى وبياناته محلاً لجرائم الإتلاف المنصوص عليها قانوناً ، وإحاطتها بالحماية المقررة فى قانون العقوبات ، أضف إلى ذلك ضرورة ووجوب سن تشريع متعلق بمثل هذا النوع من الجرائم ذات التقنية العالية وإضافة نصوص جنائية تتناسب مع وقع هذه الجريمة.

ويتمثل الركن المعنوى لهذه الجريمة فى توافر القصد الجنائى العام بعنصريه العلم والإرادة ، أى يجب أن يعلم الجانى بأنه يتلف برامج حاسب آلى خاصة بشخص آخر وذلك بإفسادها أو تخريبها أو تعطيلها ، وفى نفس الوقت تتجه إرادته لإرتكاب هذا الفعل.

أما إذا كان الإتلاف غير مقصود كما لو حدث أمر عارض أدى لإفساد برامج الحاسب الآلى ، فإن الفاعل يسأل عن خطئه أو إهماله أو تقصيره فقط.

- **وسائل إتلاف برامج وبيانات الحاسب الآلى:**

تعد فيروسات الحاسب الآلى هى الوسيلة الفعالة لإتلاف برامج الحاسب الآلى، وتعرف الفيروسات بأنها برمجيات مشفرة للحاسب الآلي مثل أي برمجيات أخرى يتم تصميمها بهدف محدد وهو إحداث أكبر ضرر ممكن بأنظمة الحاسب الآلي، وتتميز بقدرتها على ربط نفسها

بالبرامج الأخرى وإعادة إنشاء نفسها حتى تبدوا وكأنها تتكاثر وتتوالدذاتيا، بالإضافة إلى قدرتها على الانتشار من نظام إلى أخر عبر شبكات الاتصال العالمية أو بواسطة قرص ممغنط[1].

والفيروسات كما هو معلوم ليست وليدة الإنترنت فقد أشار إلى مفهوم فيروس الحاسب الآلى العالم الرياضي المعروف فون نيوتن في منتصف الأربعينات الميلادية ، إلا أن الإنترنت أصبحت الوسيلة الأكثر إستخداما في نشر وتوزيع الفيروسات في السنوات الأخيرة ، فالهدف المباشر للفيروسات هو المعلومات المخزنة على الأجهزة المقتحمة عبر شبكة الإنترنت حيث تقوم بتغييرها أو حذفها أو سرقتها ونقلها إلى أجهزة أخرى[2].

ولا بد من ملاحظة أن استعمال لفظ الفيروس هو مجازاً، فهو في الحقيقة برنامج للحاسب الآلي، وهو ليس فيروسا بالمعنى العضوي أو البيولوجي، بالرغم من أنهما يشتركان في بعض الخصائص[3].

- **سمات وخصائص الفيروسات:**

1. **القدرة على التخفي:** المقصود بالتخفى هنا هو أنه . أى الفيروس . غالباً ما قد يتخفى داخل أحد البرامج العادية التى يقوم المستخدم بتحميلها من الإنترنت معتقداً سلامة هذه البرامج وخلوها من أى أضرار.

2 . **الإنتشار:** يأتى الإنتشار مكملاً للتخفى ، فبعد قيام المستخدم بتحميل البرنامج الذى يحوى فيروساً ويثبته فى جهازه ، يبدأ الفيروس بالإنتشار والتوسع داخل الجهاز تمهيداً لقيامه بالغرض المعد لأجله سواء كان إتلاف البرامج الموجودة داخل الجهاز جزئياً أو كلياً.

3 . **القدرة على العدوى:** فالفيروس لا يصيب جهاز الشخص المجنى عليه فحسب بل قد ينتقل عبر شبكة الإنترنت إلى غيره من الأجهزة.

4 . **الإختراق:** للفيروس القدرة كذلك على إختراق البرامج المثبتة على الحاسب الآلى وإتلافها والتى قد يكون من ضمنها البرامج المضادة للفيروسات ، وهى الوظيفة التى أعد من أجلها الفيروس.

- **أنواع الفيروسات:**

1 . **برامج الدودة** : وهي عبارة عن برامج تقوم بإستغلال أية فجوة في أنظمة التشغيل لكي

---

(1) أنظر فى ذلك ، مقال بعنوان ، جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، منشور على الموقع الإليكتروني ،www.arblaws.com

(2)http://shkoon.coolfreepage.com/amn/pages/amn-jra.htm

(3) د. محمد حسين منصور، المرجع السابق، ص 292.

تنتقل من حاسب لآخر، وهذه البرامج تقوم بالقضاء على موارد الجهاز [1].

ومن الأمثلة على ذلك تمكن طالب يبلغ من العمر 23 عاما ويدعى ROBER MORRIS فى العام 1988من إطلاق فيروس عرف بإسم (دودة مورس) عبر الإنترنت ، أدى الى إصابة 6 آلاف جهاز يرتبط معها حوالي 60000 نظام عبر الإنترنت من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية ، وقد قدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار إضافة إلى مبالغ أكثر من ذلك تمثل الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة ، وقد حكم على مورس بالسجن لمدة 3 أعوام وعشرة آلاف دولار غرامة[2].

2 . **حصان طروادة** : وهو عبارة عن برنامج فيروسي لديه القدرة على الإختفاء داخل برامج أخرى أصلية للمستخدم، وتعتبر من برامج الإختراق من أجل جمع البيانات والمعلومات، وهو لا يتكاثر ولا يلتصق بالملفات وإنما هو برنامج مستقل بذاته يحمل في طياته توقيت وأسلوب استيقاظه، ولا بد من تدخل الإنسان لتنشيطه.

3. **القنبلة المعلوماتية:** وهي نوع من البرامج الخبيثة صغيرة الحجم يتم إدخالها بطرق غير مشروعة وخفية مع برامج أخرى، ويؤدي إجتماعها هذا إلى إنعدام القدرة على تشغيل برامج الحاسب الآلي ومن الأمثلة على هذا الفيروس زرع القنبلة المنطقية لتعمل لدى إضافة سجل موظف بحيث تنفجر لتمحو سجلات الموظفين الموجودة أصلا في المنشأة مثلما حصل في ولاية لوس أنجلس الأمريكية عندما تمكن أحد الأشخاص من وضع قنبلة منطقية، مما أدى إلى تخريب النظام عدة مرات[3].

4 . **القنبلة المنطقية:** هذا النوع ينشط بمجرد حدوث واقعة معينة مثل بدأ تشغيل الجهاز أو عند إنجاز أمر معين في الحاسب الآلي أو عند بدأ تشغيل برنامج معين[4].

5 . **القنبلة الزمنية:** حيث ينشط الفيروس في تاريخ معين محدد بالذات فهو يثير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة والوقت اللازم ومثال هذا الفيروس ما قام به شخص يعمل بوظيفة محاسب حيث وضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة بدافع الانتقام، وانفجرت القنبلة بعد مضي ستة أشهر من رحيله عن المنشأة وترتب على ذلك

(1) مقال جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، المرجع السابق.

(2)www.moheet.com/ show_files.aspx?fid=44439

(3) مقال جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، المرجع السابق.

(4) محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت (الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع عمان ، 2007، ص 240.

إتلاف كل البيانات المتعلقة بها[1] .

- **صور الإتلاف المعلوماتى:**

يتحقق الإتلاف المعلوماتى بصورتين الصورة الأولى تتمثل فى إدخال بيانات أو معلومات فى نظام الحاسب الآلى والمراد بذلك هو إدخال بيانات عن طريق شبكة الإنترنت فى جهاز الشخص المجنى عليه لم تكن موجودة من قبل وذلك بغرض الإضرار بجهازه وإتلافه.

أما الثانية فتتمثل فى محو أو تعديل بعض البيانات المخزنة بالحاسب الآلى، ومحو البيانات يعنى تدميرها ، أى إتلافها بصورة جزئية أو كلية والتعديل يعنى التلاعب فى هذه البيانات بشكل يؤثر فى قيمتها بحيث يتحقق معنى الإتلاف[2].

- **الموقف التشريعى من جريمة الإتلاف المعلوماتى:**

رأينا عند إستعراضنا لنصوص قانونى العقوبات المصرى والليبى أنهما قد نصا على جريمة الإتلاف ، بالطبع لم يقصدا الإتلاف المعلوماتى ولم يفردا لهذا الأخير أى نص يختص به ، ولكن . ووفقاً لما نعتقده صحيحاً . أن نصوص الإتلاف الواردة بقانون العقوبات واجبة الإعمال كما أسلفنا ، على الرغم من إعتراض جانب من الفقه على ذلك بزعم أن معطيات الحاسب الآلى هى معطيات معنوية ليست مادية ، وبالتالى تخرج من طائل القانون ، لكن حجج الفريق المؤيد لتطبيق قانون العقوبات حجج فعالة أثبتت أولوية النصوص العقابية فى مواجهة هذه الجريمة ، وإضافة لذلك . ووفقاً للمنطق . فإن هنالك حجة أخرى نضيفها لحجج الفريق المؤيد لتطبيق قانون العقوبات ، وهى أن المعطيات والبرامج الخاصة بالحاسب الآلى حتى وإن كانت معنوية ليست مادية فهى كذلك تستوجب الحماية الجنائية على أساس أنها . أى البرامج . مملوكة للغير وبالتالى وجبت حماية هذا الغير وحماية ملكيته سواء ما كان يملكه ذو قيمة مادية أو معنوية وهذا ما أكده القانون رقم 82 لسنة 2002 بشأن إصدار قانون حقوق الملكية الفكرية فى مصر والذى نص فى مادته رقم 140 فى الفقرتين 2،3 على أنه: " تتمتع بحماية هذا القانون حقوق المؤلفين على مصنفاتهم الأدبية والفنية وبوجه خاص المصنفات الاتية:

2. برامج الحاسب الآلى.

3. قواعد البيانات سواء كانت مقروءة من الحاسب الآلى أوغيره ".

وهو ذات النهج الذى إنتهجه المشرع الليبى فى مشروع قانون حماية حقوق المؤلف والحقوق المجاورة.

---

(1) وجدي عبد الفتاح سواحل، المرجع السابق.

(2) د. هدى حامد قشقوش ، المرجع السابق ، ص 569.

هذا بالإضافة لضرورة إضافة نصوص عقابية أو سن تشريعات خاصة بالمعالجة غير المشروعة لبيانات الحاسب الآلى أو سن تشريع خاص بهذه الجريمة وجرائم الإنترنت بشكل عام.

أما نظام مكافحة الجرائم المعلوماتية فقد نص فى مادته الخامسة فقرة 1 على أنه "يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال ، أو بإحدى هاتين العقوبتين كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

الدخول غير المشروع لإلغاء بيانات خاصة ، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، أو إعادة نشرها".

وقد جرّمت اتفاقية بودابست الإتلاف الذي تتعرض له برامج الحاسب الآلي ونصت على عدة صور يتم بها الإتلاف المعلوماتي كالإتلاف والإفساد والتدمير والتعديل أو محو البيانات فى المادتين 4 ، 5. حيث نصت فيهما على ضرورة قيام كل دولة طرف فى الإتفاقية على إتخاذ تدابير تشريعية لتجريم تلك الأفعال.

المطلب الثالث

جرائم غسيل الأموال عبر الإنترنت

تعتبر جرائم غسيل الأموال (Money Laundering) أخطر جرائم التكنولوجيا الرقمية ، وتعود الجذور الأولى لجريمة غسيل الأموال إلى عصابات المافيا التى كانت تمارس أنشطة عديدة غير مشروعة كتجارة الأسلحة والمخدرات والدعارة والإبتزاز والقمار ، الأمر الذى أدى بها إلى محاولة تبييض أو غسيل الأموال المتحصلة عن تلك الأنشطة وذلك بإضفاء صفة الشرعية عليها .

وكان أحد أبرز الطرق لتحقيق هذا الهدف شراء الموجودات وإنشاء المشاريع ، وهو ما قام به أحد اشهر قادة المافيا (آل كابون)[1].

الفرع الأول

التعريف بجريمة غسيل الأموال

برز مصطلح غسيل الأموال على الساحة الإقتصادية في المجال القانوني لأول مرة في إحدى القضايا بالولايات المتحدة الأمريكية عام 1982 وكانت هذه القضية قد اشتملت على مصادرة أملاك تم غسيلها في عمليات الكوكايين الكولومبية ، وقد بدأ الإهتمام الدولي بموضوع غسيل الأموال منذ إبرام اتفاقية الأمم المتحدة لمكافحة الإتجار غير المشروع في المخدرات والمؤثرات العقلية فيينا 1988 خاصة في المادة الخامسة من الإتفاقية التي نصت على مصادرة أرباح وثروات المشتغلين بالإتجار غير المشروع في تلك الأنشطة والتي تمكن المنظمات الإجرامية غير الوطنية من إختراق وتلويث وإفساد هياكل الحكومات والمؤسسات التجارية والمالية المشروعة على كافة المستويات[2].

وقد نص في المادة الثالثة من الإتفاقية المذكورة على أن غسيل الأموال يتمثل إما في تحويل الأموال أو نقلها مع العلم بأنها من نتاج جرائم المخدرات ، أو في إخفاء أو تمويه حقيقة الأموال أو مصدرها أو في إكتساب أو حيازة أو إستخدام الأموال مع العلم وقت تسليمها أنها من

---

(1) المحامى يونس عرب ، مقال بعنوان ، جرائم غسيل الأموال، دراسة في ماهية ومخاطر جرائم غسيل الاموال والاتجاهات الدولية لمكافحتها ، راجع الموقع
www.foca.net/AR/Money_Laundry_Crimes.doc

(2) إنعام محسن غدير / سارة مشير عبد الهادي ، مقال بعنوان ، غسيل الأموال .. مراحله . طرقه والآثار الناجمة عنه ، راجع الموقع
http://www.free-pens.org/index.php?show=news&action=article&id=141

حصيلة جريمة من الجرائم المنصوص عليها فى هذه الإتفاقية.

وكذلك بينت الفقرة الأولى من المادة السادسة من إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، مفهوم جريمة غسيل الأموال، بأنه "أية أفعال ترتكب عمدًا، لتحويل الممتلكات أو نقلها، مع العلم بأنها عائدات جرائم بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات، أو إخفاء وتمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو ملكيتها أو الحقوق المتعلقة بها، مع العلم بأنها عائدات جرائم."

تعريف جريمة غسيل الأموال فى القانون رقم 80 لسنة 2002 والمعدل بالقانون رقم 78 لسنة 2003:

عرف القانون رقم 80 لسنة 2002 والمعدل بالقانون رقم 78 لسنة 2003 فى مصر، فى المادة الأولى فقرة (ب) جريمة غسيل الأموال بأنها كل سلوك ينطوى على إكتساب أموال أو حيازتها أو التصرف فيها أو إدارتها أو حفظها أو إستبدالها أو إيداعها أو ضمانها أو إستثمارها أو نقلها أو تحويلها أو التلاعب فى قيمتها إذا كانت متحصلة من جريمة من الجرائم المنصوص عليها فى المادة (2) من هذا القانون مع العلم بذلك ، متى كان القصد من هذا السلوك إخفاء المال أو تمويه طبيعته أو مصدره أو مكانه أو صاحبه أو صاحب الحق فيه أو تغيير حقيقته أو الحيلولة دون اكتشاف ذلك أو عرقلة التوصل الى شخص من إرتكب الجريمة المتحصل منها المال.

تعريف جريمة غسيل الأموال فى القانون رقم (2) لسنة1373و.ر2005م بشأن مكافحة غسيل الأموال:

عرفت جريمة غسيل الأموال فى ليبيا وفقاً للقانون رقم (2) لسنة1373و.ر2005م فى المادة الثانية منه ، وذلك على النحو التالى:

أولاً : يعد مرتكباً جريمة غسيل الأموال كل من أتى سلوكاً من أنماط السلوك التالية:

أ – تملك الأموال غيرالمشروعة ، أو حيازتها أو إستعمالها أو إستغلالها، أو التصرف فيها على أي وجه، أو تحويلها أو نقلها أو إيداعها أو إخفاؤها، بقصد تمويه مصدرها غير المشروع .

ب– تمويه حقيقة الأموال غير المشروعة ، أو إخفاء مكانها أو طريقة التصرُّف فيها أو حركتها، أو الحقوق المُتعلِّقة بها أو ملكيتها أو حيازتها .

جـ – الإشتراك فيما سبق بأي صورة من صور الإشتراك .

ثانيا : تكون الأموال غير مشروعة إذا كانت مُتَحَصلة من جريمة

بما في ذلك الجرائم المنصوص عليها في الإفاقية الدولية لمكافحة الجريمة المنظمة ، والبروتوكولات الملحقة بها ، والإتفاقية الدولية لمكافحة الفساد، وغيرهما من الإتفاقيات الدولية ، ذات الصلة ، التي تكون الدولة طرفاً فيها .

- **مراحل عملية غسيل الأموال[1]:**

المرحلة الأولى:

عملية إدخال المال في النظام المالي القانوني (PLACEMENT) ، وهدف هذه المرحلة التخلص من كمية النقد الكبيرة بين يدي مالكها وتحويلها إلى أشكال نقدية أو مالية مختلفة كالشيكات السياحية والحوالات البريدية وغيرها.

المرحلة الثانية:

وهي عملية نقل وتبادل المال القذر ضمن النظام المالي الذي تم إدخالها فيه (LAYERING) وهى المرحلة التى يبدأ فيها الجناة بخلق عمليات معقدة بهدف التمويه عن مصدر تلك الأموال.

المرحلة الثالثة:

تتمثل بعملية دمج المال نهائيا بالأموال المشروعة لضمان إخفاء المصدر القذر لها (INTEGRATION).

- **خصائص جريمة غسيل الأموال [2]:**

1 . جريمة غسيل الأموال جريمة لاحقة وضرورية لجريمة أصلية : أي أنه لقيام جريمة غسيل الأموال لابد من وجود جريمة سابقة عليها أدت إلى الحصول على كمية من الأموال غير المشروعة و بالتالي لمحاربه جريمة غسيل الأموال لابد من التركيز على مكافحة الجرائم الأصلية التي تنتج عنها الأموال الغير مشروعة.

2 . جريمة غسيل الأموال جريمة ذات طابع دولي: أي أنه يمكن أن ترتكب الجريمة الأصلية التي ينتج عنها أموال غير مشروعة في بلد معين ويتم نشاط غسيل الأموال في بلد آخر.

3 . جريمة غسيل الأموال جريمة ذات طابع إقتصادي : جريمة غسيل الأموال يترتب عليها إضفاء طابع المشروعية على الأموال غير المشروعة المتحصلة من جرائم معينة، وما

---

(1) راجع بهذا الخصوص المحامى يونس عرب ، المقال السابق.

(2) راجع فى خصوص ذلك ، مقال بعنوان غسيل الأموال تعريفها وخصائصها ، الموقع الاليكترونى http://www.titanic-arwad.com/vb/showthread.php?t=13866

يستتبعه من آثار سلبية على الدخل القومي والناتج القومي وعلى أنماط الإستهلاك، والإدخار، والإستثمار، وقيمة العملة الوطنية، وذلك نتيجة إندماج الأموال غير المشروعة في الإقتصاد الرسمي للدولة ، فإن جريمة غسيل الأموال تعتبر من الجرائم الإقتصادية الخطيرة.

4. جريمة غسيل الأموال متطورة فنيًا وتقنيًا: حيث أدت التطورات التكنولوجية مثل ظهور النقد الرقمي وتطور أنظمة التحويلات المالية إليكترونيًا، وإنتشار التجارة الإلكترونية، ونمو العلاقات بين البنوك و تزايد إستخدام شبكة الإنترنت ، إلى السرعة فى تنفيذ الجريمة في أقل وقت ممكن .

5. جريمة غسيل الأموال جريمة منظمة أي لا يقتصر إرتكاب جريمة غسيل الأموال على صغار المجرمين، بل إنه يتم إرتكابها من قبل جماعات وعصابات منظمة قوية يتخطى نشاطها الحدود الوطنية.

- **أركان جريمة غسيل الأموال:**

أولا: الركن المادي:

من خلال مراجعة موقف كلاً من المشرعين المصرى والليبى ، فإن الركن المادى لجريمة غسيل الأموال يتمثل فى:

أ . جريمة أولية تعد هى المصدر الأصلى لهذه الأموال محل الجريمة.

ب . أن يكون المال المتحصل من الجريمة غير مشروع ويخشى الجانى الإفصاح عن مصدره.

جـ . قيام الجانى بإدخال تلك الأموال فى النظام القانونى للأموال محاولاً إضفاء صفة الشرعية عليه.

ثانياً: الركن المعنوى:

تعد جريمة غسيل الأموال من الجرائم العمدية التي تقوم على القصد الجنائي العام بعنصريه العلم والإرادة ، والقصد الجنائي العام في هذه الجريمة ينصرف إلى علم الجاني بأنه يمارس نشاطاً غير مشروع – غسيل الأموال – بأموال أو عائدات من نشاط غير قانوني، ومع ذلك تتصرف إرادته إلى إرتكاب هذا السلوك الإجرامي وكذلك قبول النتائج المترتبة عليه، وهو ما يعبر عنه في القواعد العامة لقانون العقوبات بنظرية العلم ونظرية الإرادة، أي العلم بحقيقة السلوك الإجرامي وحظر المشرع له، ومع ذلك تتصرف الإرادة إلى إتيان السلوك الإجرامي وقبول النتائج المترتبة عليه.

الفـــرع الثانـــى
أساليب غسيل الأموال عبر شبكة الإنترنت

أخذت جريمة غسيل الأموال بعداً جديداً مع إنتشار وإزدياد التقدم التكنولوجى على مستوى العالم ، وهو الأمرالذى يعتبر قد ساهم فى إرتكاب هذه الجريمة بشكل أسرع وأئمن من خلال تكنولوجيا شبكة الإنترنت ، وتعدد الأساليب المتبعة لغسيل الأموال عبر شبكة الإنترنت كما يلى:

1 ـ العمليات المصرفية عبر الإنترنت:

تزخر شبكة الإنترنت بالعديد من البنوك والمصارف التى تقدم خدماتها عبر الشبكة ، وإضافةً لذلك توجد بعض المؤسسات المالية التى تقدم بعض الخدمات التى قد تعتبر بنكية ، وهو ما قد يستغله بعض الجناة كوسيلة سهلة وميسرة لغسيل أموالهم القذرة. ويتم غسيل الأموال من خلال بنوك الإنترنت على النحو التالى:

أ . فتح حساب فى إحدى بنوك الإنترنت، وذلك عن طريق إستمارة تملى عن طريق الإنترنت، وفيها يضع العميل إسمه والذى غالباً ما يكون إسم وهمى، وقد بفتح الجانى حساباً واحداً أو عدة حسابات فى نفس البنك أو فى عدة بنوك منتشرة حول العالم.

ب . الإيداع : وذلك عن طريق الإيداع النقدى أو الإليكترونى أو بكلتا الطريقتين.

جـ . بعد إيداع الأموال فى البنك تأتى المرحلة الأهم وهى مرحلة إختلاط أموال الجانى بالأموال الموجودة بالبنك والخاصة بعملاء هذا الأخير وقيامه بإستثمارها فى عديد المشروعات المختلفة ، ويتم إستغلال المال كوحدة واحدة في الإستثمار.

إضافةً لذلك فإن الجانى قد يستطيع الحصول على قروض بضمان هذه المبالغ المودعة وهو أمر يدر على البنك ربحاً متحصل من الفوائد المحتسبة على قيمة القرض، بل ويمكن أن يتم الإقتراض من بنك آخر بضمان الوديعه، وقد يكون هذا البنك في دولة أخرى غير دولة البنك المودع لديه، والأموال المقترضه هي بطبيعة الحال أموال نظيفة يمكن من خلالها الإشتراك في مشروعات أو شراء ممتلكات تبدو في صورة مشروعة تماما.

د . السحب الإلكتروني: يمكن لصاحب الحساب أن يحصل من البنك المودع لديه على كارت ممغنط (atm) يستطيع بموجبه أن يسحب الأموال إلكترونيا من أي مكان في العالم.

هـ . التحويل الإليكترونى: كذلك قد يستطيع غاسل الأموال تحويل الأموال من بنوك الإنترنت

إليكترونياً إلى أى حساب آخر فى الداخل أو الخارج.

2 ـ التجارة الإلكترونية:

قد يستطيع الشخص غاسل الأموال كذلك غسيل أمواله القذرة عن طريق المتاجرة الإليكترونية ، وذلك بعقد صفقات ضخمة عبر شبكة الإنترنت يقوم من خلالها بشراء بضائع ومنتجات ثمينة ثم يقوم بإعادة طرحها للبيع وإظهار المال القذر بمظهر المال النظيف المتأتى من تجارة مشروعة.

3ـ المقامرة عبر الإنترنت:

مع إنتشار شبكة الانترنت على مستوى العالم فقد أصبح لعب القمار أسهل نظراً لأن اللاعبين بات بإمكانهم اللعب وكل في مسكنه وكثيراً ما تتداخل عملية غسيل الأموال مع أندية القمار المنتشرة على شبكة الإنترنت ، الأمر الذي جعل مواقع الكازينوهات الإفتراضية تنمو بشكل كبير على شبكة الإنترنت ، و المشكلة القانونية فى هذه المواقع أنها إفتراضية وليس لها مكان معلوم، على عكس نوادي القمار الحقيقية[1].

ولقد قامت مجموعة العمل المالية (FATF) وهى مجموعة عمل مالى دولى مختصة بدراسة أسباب ووسائل وطرق مكافحة غسيل الأموال ، ولقد انبثقت هذه المجموعة عن قمة (L`arche) التى عقدت فى باريس فى يوليو من العام 1989[2].

قامت هذه المجموعة بإعداد تقرير تم نشره في فبراير 2001 ، أشارت فيه إلى أن "المقامرة على شبكة الإنترنت، ربما تكون خدمة نموذجية لكي تكون غطاء لمخطط غسيل أموال عن طريق شبكة الإنترنت، وأن المجرمين يستخدمون صناعة القمارعلى شبكة الإنترنت لإرتكاب الجرائم ولغسيل عوائد الجريمة. وفي يونيو 2003، فإن فريق العمل المكلف باتخاذ إجراءات مالية حول غسيل الأموال والمنظمة الدولية المتعددة الأطراف لمكافحة غسيل الأموال، قد اعترفا بالمشكلة التي تزداد تفاقما والتي يمثلها القمار على شبكة الإنترنت وقامت بمراجعة توصياتها الأربعين بخصوص مكافحة غسيل الأموال، لكي تتضمن، من بين أشياء أخرى، التوصيات التي تؤثر على الكازينوهات، والكازينوهات التي تتضمنها شبكة الإنترنت تحديدا[3].

---

(1) د. محمد ياسر أبو الفتوح ، مقال بعنوان خصائص وتصنيفات الجريمة المعلوماتية ، راجع الموقع http://www.shaimaaatalla.com/vb/showthread.php?t=3951

(2) راجع فى نفس المعنى ، محمد عبد الله ابو بكر سلامة ، المرجع السابق ، ص205.

(3)http://www.bcblebanon.com/arabic/court_cases/internet_banks_fraud.htm#_Toc100725665

4 ـ المضاربة فى سوق الأوراق المالية:

وسيلة أخرى لغاسل الأموال يستطيع من خلالها تبييض أمواله ، وذلك عن طريق الدخول فى سوق الأوراق المالية والبورصة عبر الإنترنت حيث يقوم بشراء عديد كبير من الأسهم وبمبالغ هائلة ثم يعود بعد ذلك ويقوم ببيعها.

ولو أمعنا النظرفى جميع طرق غسيل الأموال عن طريق الإنترنت ، لوجدنا أنها ترتكز جميعاً على وجود رصيد إليكترونى مودع لمصلحة الجانى فى إحدى البنوك التى تتعامل عن طريق الإنترنت . بغض النظر كان هذا الرصيد بإسمه أولا . ويستطيع من خلاله تحويل أمواله أو التجارة عن بعد أو شراء الاسهم فى البورصة وكذلك المقامرة.

ومن الملاحظ كذلك . وفقاً لما نعتقد بصحته . أن هناك فارق يستحق الذكربين جريمة غسيل الأموال و الجرائم الواقعة على التجارة الإليكترونية ، فجرائم التجارة الإليكترونية يتميز الجانى فيها بأنه يسعى إلى الوصول إلى منفعة مادية من خلال سلوكه الإجرامى المتمثل فى النصب أو السرقة أو الإعتداء على حقوق الغير للحصول على منفعته ، أى إنه يسعى لإنتزاع ضالته من خلال شبكة الإنترنت ، فالمال محل السرقة أو النصب أو الإعتداء كائن داخل شبكة الإنترنت ، أما فى جرائم غسيل الأموال عبر الإنترنت فإن الأمر يختلف فالجانى هنا قد تحصل على المنفعة المادية المتمثلة فى مبلغ مالى من نشاط غير قانونى أو غير مشروع ولكنه يسعى جاهداً لإدخال هذا المال فى المنظومة الإقتصادية أو التجارية للشبكة من أجل دورانه فيها وغسيله ومن ثم إستعادته مالاً مشروعاً، ومن الممكن كذلك أن يكون المال المتحصل من جرائم التجارة الإليكترونية محلاً لغسيله عن طريق الإنترنت ، وذلك بقيام المجرم الذى تحصل على المال من خلال الشبكة بإدخاله من جديد فى الشبكة بإحدى الطرق لإضفاء عليه وصف المشروعية.

ومن أبرز الأمثلة لغسيل الأموال عن طريق الإنترنت ، قيام السلطات المصرية بالقبض على 43 شخص لإرتكابهم خارج مصر وداخلها جريمة غسيل أموال تبلغ قيمتها مليونا و117 ألف دولار أمريكى متحصلة من جرائم نصب حيث تلقى 11 متهماً جزءاً من الأموال عن طريق عدة تحويلات من الخارج، وصرفوها من إحدى شركات تحويل الأموال داخل مصر، وأودعوها حسابات أحد المتهمين بعدة بنوك وصندوق توفير البريد بهدف إخفاء مصدر الأموال وعرقلة التوصل إلى مرتكبى الجريمة وقد أوضحت نيابة أمن الدولة العليا أن المتهمين إشتركوا فيما بينهم بطريقى الإتفاق والمساعدة فى إرتكاب جريمة غسيل الأموال، بأن إتفق عدد منهم على تلقى التحويلات المالية الواردة من الخارج بأسمائهم، والمتحصلة من جريمة نصب، وصرفوها

عبر فروع إحدى شركات تحويل الأموال، حيث أمدوا بعضهم بعضاً بمعلومات وتواريخ ورود هذه التحويلات من الفروع الواردة عليها لصرفها وتوزيعها فيما بينهم[1].

الفرع الثالث

الموقف التشريعى من جرائم غسيل الأموال عبر الإنترنت:

فى مصر نص القانون رقم 80 لسنة 2002 والمعدل بالقانون رقم 78 لسنة 2003، فى المادة 14 على أنه: يعاقب بالسجن مدة لا تجاوز سبع سنوات وبغرامة تعادل مثلى الأموال محل الجريمة ، كل من إرتكب أو شرع فى إرتكاب جريمة غسيل الأموال المنصوص عليها فى المادة (2) من هذا القانون . ويحكم فى جميع الأحوال بمصادرة الأموال المضبوطة ، أو بغرامة إضافية تعادل قيمتها فى حالة تعذر ضبطها أو فى حالة التصرف فيها إلى الغير حسن النية.

وقد تضمن القانون سالف الذكر بعض الضوابط الرقابية التى يتعين أن تلتزم بها البنوك والمؤسسات المالية بشأن مكافحة غسيل الأموال فيما يتعلق بفتح حسابات الزبائن من حيث التعرف على هوياتهم والتأكد من بياناتهم وضرورة الإخطار عن العمليات التى يشتبه فى إنها تتضمن غسيل أموال ، وكذلك التحكم فى النقد الأجنبى الوارد إلى مصر من حيث معرفة مقداره حال مجاوزته العشرين ألف دولارأو مايعادل ذلك. وقد إنضمت مصر للإتفاقية العربية لمكافحة الإتجار غير المشروع بالمخدرات والمؤثرات العقلية تونس1994، وإنضمامها كذلك لمجموعة الإيجمونت فى عام 2004 ، وهى تجمع دولى تشارك فيه وحدات غسيل الأموال بدول العالم حتى يمكن تبادل المعلومات اللازمة وتنسيق الجهود لمكافحة جريمة غسيل الأموال فى كافة الدول الأعضاء بتلك المنظمة .

أما فى ليبيا فقد نص القانون رقم (2) لسنة1373و.ر2005م بشأن مكافحة غسيل الأموال فى مادته الرابعة على عقوبة غسيل الأموال بالآتى:

<u>**أولاً**</u> : مع عدم الإخلال بالعقوبات المنصوص عليها في قانون العقوبات أو أى قانون آخر ، والمُقَررة للجرائم التي تكون مصدراً للأموال غير المشروعة ،يعاقب على جريمة غسيل الأموال ، المنصوص عليها في الفقرة (أولاً) من المادة الثانية ، بالسجن وبغرامة تعادل قيمة المال محل الجريمة ، مع مصادرة المال.

---

(1) http://www.egypty.com/accidents-details.aspx?accidents=3030

وإذا كان الجاني مساهماً في الجريمة المُتحصلة منها الأموال ، سواء بوَصْفه فاعلاً أو شريكاً ، عوقببَ بعقوبة الجريمة ذات الوصف الأشد ، مع زيادة حديْها إلى الثلث .

أما إذا كان الجاني يعلم أن الأموال مُتحصلة من جريمة عقوبتها أشد ، دون أن يكون مساهماً فيها ، فتوقع عليه العقوبة المُقررة لتلك الجريمة.

ثانياً : تعاقب المنشأة التي ترتكب الجريمة بإسمها أو لحسابها بغرامة تعادل ضعف المال محل الجريمة ، مع مصادرة المال . وفي حالة العوْد يحكَم ، بالإضافة إلى ذلك ، بسحب الترخيص وغلق المنشأة.

وكذلك نص القانون على إنشاء وحدة بالمصرف المركزي تسمى " وحدة المعلومات المالية " لمواجهة عمليات غسيل الأموال، وكذلك إلزام كل مصرف من المصارف العاملة في الدولة بإنشاء وحدة فرعية تسمى "الوحدة الفرعية للمعلومات المُتعلقة بمكافحة غسيل الأموال" ، تتولى رصد ومُتابعة كافَّة العمليات والصفقات التي يُجريها المصرف أو المُؤسَّسة المالية.

وكذلك نشأت بمُوجب هذا القانون لجنة تسمى اللَّجنة الوطنية لمكافحة غسيل الأموال تقوم بإقتراح الأنظمة والإجراءات اللازمة لمكافحة غسيل الأموال.

وبعد أن عرضنا لكل من موقف المشرع المصرى ثم الليبى فى التصدى لجريمة غسيل الأموال ، فإنه من الملاحظ عدم إشارة أياً منهما لجرائم غسيل الأموال التى تتم عبر الإنترنت ، حيث عبرا عن جريمة غسيل الأموال بشكل عام وهو مايمكن معه القول بصحة إنطباق النصين سالفى الذكر أيا كانت طريقة إرتكاب الجريمة مع ضرورة إضافة نصوص خاصة بها تعرف الجريمة وكيف ترتكب عبر شبكة الإنترنت ووضع العقوبات التى تتلائم مع خطورتها وخطورة مرتكبيها، وذلك نظراً لتعاظم دور شبكة الإنترنت فى تسهيل إرتكاب هذه الجريمة التى سبق وأن رأينا تميزها بالطابع المنظم والدولى فى نفس الآن مما يزيد من صعوبتها على المشرع الوطنى خاصةً فيما يتعلق بمكان إرتكابها وموقع الجانى ، لذا وجب تشديد الرقابة على العمليات المصرفية التى تتم عبر الإنترنت من قبل البنوك التى تتعامل فى هذا المجال.

أما عن المجهودات الدولية المبذولة لمكافحة جريمة غسيل الأموال فقد تعددت ويأتى على رأسها: بيان بازل عام 1988 ، إتفاقية باليرمو فى العام 2000 ، ميثاق السيطرة على عمليات غسل الاموال بين البنوك العالمية فى العام 2000 ، لجنة العمل المالى الدولى لمكافحة غسيل الأموال لجنة فاتف (F.A.T.F) ، إتفاقية الأمم المتحدة لمكافحة الفساد فى العام 2003.

الفصل الثانى
مكافحة جرائم الإنترنت

تمهيد وتقسيم:

لما كانت شبكة الإنترنت من الخدمات التى تعتبر حديثة نوعاً ما فى . دول العالم العربى تحديداً . فإن أغلب الجرائم المرتكبه عبرها لم تحظى بتشريع خاص يجرمها ، ومرجع ذلك هو حداثة هذه الخدمة كما ذكرنا ، وكذلك التطور السريع والمتنامى فى أساليب إرتكابها، ونظراً لأن جريمة الإنترنت هى جريمة تتعدى الحدود الوطنية أى أن أثرها يتعدى حدود الدولة المرتكب فيها الفعل الإجرامى فإن مكافحتها كذلك لا يمكن أن تكون إلا بتكاتف الجهود الوطنية ووقوفها جنباً إلى جنب مع تلك الجهود الدولية لتدارك الموقف والحيلولة دون استشراء هذه الظاهرة وهذه الجهود أو وسائل التصدى والمكافحة هى محور بحثنا فى الفصل الثانى من هذه الدراسة وذلك على النحو التالى:

المبحث الأول : مكافحة جرائم الإنترنت على الصعيد الوطنى.

المبحث الثانى : مكافحة جرائم الإنترنت على الصعيد الدولى.

المبحـــث الأول

مكافحة جرائم الإنترنت على الصعيد الوطنى

تمهيد وتقسيم:

تسعى كل دولة لمحاربة جرائم الإنترنت داخل إقليمها راصدة لذلك عتادها الفنى والتقنى والبشرى ، فعلى المستوى التقنى والفنى يتم الإستعانة بأفضل وأحدث طرق التكنولوجيا لحماية شبكة الإنترنت من الإنتهاكات التى تحدث نتيجة إستغلال الشبكة للنفاذ داخلها وإستعمالها فيما يحظره القانون ، أما على المستوى البشرى فيتم ذلك بالإستفادة من المتخصصين فى مجال الحواسيب وشبكات الإنترنت ، إضافةً إلى المجهودات الشرطية المكثفة لقمع أو محاولة وأد هذه الأفعال وبناءً على ماسبق فإن دراستنا هذا المبحث ستكون على النحو التالى:

المطلب الأول : سبل الحماية الفنية فى مواجهة جرائم الإنترنت.

المطلب الثانى: التصدى الشرطى لجرائم الإنترنت.

المطلـــب الأول
سبل الحماية الفنية فى مواجهة جرائم الإنترنت

تتعد سبل الوقاية أو الحماية بالطرق الفنية فى مواجهة جرائم الإنترنت وتنحصر هذه الطرق فى :

أولاً : إستخدام كلمة السر.

ثانياً : تشفير البيانات.

ثالثاً : إستخدام التوقيع الإليكترونى.

رابعاً : تنقية البيانات.

خامساً : برامج الحماية.

أولاً: إستخدام كلمة السر(كلمة المرور):

كلمة السر هي سلسلة من الأحرف والأرقام تتيح الدخول إلى أحد أجهزة الكمبيوتر والوصول إلى محتوياته أو هى التى تستخدم فى الدخول إلى البريد الإليكترونى ، وتقدم كلمة السر المساعدة لضمان عدم وصول الأشخاص إلي محتويات الكمبيوتر إلا إذا تم تخويلهم ذلك، ويجب دائماً إنشاء كلمات سر قوية للحفاظ على الكمبيوتر آمناً، ويجب كذلك عدم إظهار كلمة المرور أو كتابتها في مكان ما حيث يمكن أن يراها الآخرين.

ويشترط فى كلمة السر لكى تكون فعالة

- أن تكون طويلة
- أن تكون منوعة فيما بين الأحرف الأبجدية والأرقام والرموز

. إستخدام لوحة المفاتيح كاملة فى كتابة كلمة السر.

- إستخدام كلمات وعبارات يسهل تذكرها، ولكن يصعب على الآخرين كشفها.
- عدم إستعمال إسم الشخص الحقيقى أو عنوانه ، أو رقم الهاتف ، أو معلومات شخصية أخرى ككلمة سر.
- تغيير كلمة السر بشكل دورى لضمان عدم إنكشافها أو سرقتها.

والجدير بالذكر كذلك أن إستخدام كلمة السر قد يكتنفه بعض المخاطر والتى تتمثل فى الإستيلاء عليه من مالكه وذلك عن طريق تخمين كلمة السر التى قد تتكون من معلومات شخصية كالإسم أو تاريخ الميلاد أو رقم التليفون الشخصى.

ومن طرق الحصول على كلمة السر الخاصة بالغير كذلك هو الوقوف مثلاً وراء الضحية أثناء كتابته كلمة السر، وكذلك القيام بتركيب برنامج صغير فى جهاز الحاسب الألى يسجل جميع الحروف والأرقام التى تم إستخدامها فى لوحة المفاتيح، أو إستخدام البرامج التى تقوم بتخمين كلمات المرور.

ثانياً: تشفير البيانات:

يُعرَّف التشفير بأنه عملية تحويل المعلومات إلى شيفرات غير مفهومة (تبدو غير ذات معنى) لمنع الأشخاص غير المُرخَّص لهم من الإطلاع على المعلومات أو فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مُشفَّرَة[1].

وتتألف عملية التشفير من ثلاثة عناصر،هي[2]:

1 . المعلومات التي ستجرى لها عملية تشفير وقد تكون رسالة نصية، أو ملفات مهمة، أو إشارات كهربائية مشفرة كإشارة البث التلفزيوني الرقمي.

2 . خوارزمية التشفير التي ستطبّق على المعلومات لتحويلها إلى بياناتٍ مبهمة، وخوارزمية فك التشفير التي تعيد هذه البيانات إلى حالتها المفهومة الأصلية. وهذه الخوارزميات عبارة عن دوال رياضية محددة، يزداد عامل الأمان الذي توفره، بإزدياد تعقيدها، حيث يكون فكها أو استنتاجها، صعباً للغاية .وتوجد العديد من الخوارزميات المتبعة في عمليات التشفير عبر إنترنت، منها DES و RSA وPGP.

3 . المفتاح، وهو سلسلة أو أكثر من الرموز تتسلمها الخوارزميات المتبعة، وتطبقها على البيانات لتشفيرها أو فك التشفير عنها. وتتبع أنظمة التشفير أسلوبين مختلفين، تبعاً للمفاتيح المستخدمة:

<u>أولاً</u> : تشفير المفتاح السري (SKE (secret-key encryption ، ويستخدم هذا النظام المفتاح ذاته في عمليتي التشفير وفك التشفير .ويعتمد مبدأ هذا النوع على إتفاق الطرفين المرسل والمستقبل للمعلومات المشفرة، على مفتاح سري واحد. ويعتبر عامل أمان هذا النوع أضعف من عامل أمان تشفير المفتاح العام، حيث يمكن أن يتطفل شخص معين على عملية تبادل المعلومات، التي يتم خلالها الاتفاق على المفتاح السري، ويتعرف على هذا المفتاح .ويعتبر مثال تشفير يوليوس قيصر ضمن هذا النوع من التشفير، فهو يعتمد

([1]) http://www.itep.ae/arabic/EducationalCenter/Articles/Encryption_01.asp

([2]) مقال بعنوان ، تشفير البيانات فى إنترنت ، راجع الموقع
http://www.arabteam2000-forum.com/index.php?showtopic=5441

على مفتاح واحد في عمليتي التشفير، وفك التشفير. ويعرف هذا النوع كذلك، بالتشفير المتناظر ويعتبر نظام DES (Data Encryption Standard) أشهر الأنظمة التي تعتمد على هذا النوع من التشفير، وقد طورته شركةIBM .

ثانياً : **نظام المفتاح العام PKE (public-key encryption)** ، ويستخدم زوجاً من المفاتيح: أحدهما يدعى المفتاح العام، ويتم الإعلان عنه لجميع الجهات التي تتبادل المعلومات، وهو المفتاح المستخدم لتشفير البيانات، والآخر يدعى المفتاح الخاص، وهو المستخدم لفك التشفير، ويبقى هذا المفتاح سراً عند الجهة المستقبلة، فتزول بذلك، ضرورة تبادل المرسل والمستقبل المفتاح، الذي قد يتعرض للكشف خلال عملية التبادل.

وتعتمد بعض الشركات التى تقدم خدمات تجارية بواسطة بطاقات الإئتمان على شبكة الإنترنت أسلوب التشفير لحماية عملياتها التجارية ، كشركتى ماستر كارد وفيزا كارد ، ومع ذلك فإن للتشفير خطورته حيث أنه يجعل مهمة البوليس مستحيلة لأنه يمنعه من إكتشاف الجرائم التى تتضمنها الحاسبات الآلية ، وخاصة بالنسبة للإرهابيين ومروجى الصور ذات الطابع الإباحى[1].

ثالثاً: إستخدام التوقيع الإليكترونى:

يعتبر التوقيع الإليكترونى طريقة من طرق الإتصال المشفرة التى تعمل على توثيق المعاملات التى تبرم عبر الإنترنت وللتوقيع الإليكترونى عدة مميزات وفوائد تلخص فى الآتى:

- يشير التوقيع الإليكترونى إلى شخص محدد بالذات وينسب التصرف القانونى الصادر إليه وحده دون غيره وذلك عن طريق كلمات سر معينة أو بطاقات ذكيه وكذلك عن طريق شهادات التصديق الإليكترونية التى تشير إلى الشخص صاحب التوقيع دون غيره.
- وكذلك يحمى التوقيع الإليكترونى سرية البيانات والمعلومات وسلامتها بحيث يمنع الغير من الإطلاع عليها أو محاولة إستخدامها أو محاولة تغيير محتواها، وكذلك حماية المؤسسات من عمليات التزييف وتزوير التوقيعات.
- يحقق التوقيع الإليكترونى ضمانة أخرى هامة ألا وهى عدم مقدرة الشخص صاحب التوقيع الإليكترونى ، على إنكار قيامه بالمعاملة التجارية الإليكترونية وذلك لوجود جهة التصديق سالفة الذكر التى توثق كافة المعاملات وكذلك عدم قدرة الشخص المستفيد من التوقيع على إنكار المعاملة.

---

(1) د. طارق إبراهيم الدسوقى عطية ، الأمن المعلوماتى (النظام القانونى للحماية المعلوماتية) ، دار الجامعة الجديدة ، 2009 ، ص 586 . 587.

رابعاً: تنقية المعلومات:

تنقية المعلومات هى وسيلة تمكن المؤسسات أو الأفراد من حجب الوصول إلى بعض محتويات الشبكة العنكبويته والتي يرون أنها غير مناسبة للمستخدم ، أوهى آلية تستخدم لحصر الوصول إلى محتويات شبكة الإنترنت بناءً على مصدر هذه البيانات.

وتتم طريقة عمل هذا النظام بعدة طرق من أبرزها:

1- فلترة المعلومات بناء على مصدرها:

وهذه الطريقة تستدعي حجب المعلومات المستقبلة أو المرسلة من مصادر معينة تم تصنيفها مسبقا على أنها غير مقبولة.وفلترة المعلومات بناءً على مصدرها يتم بصورتين:

- الصورة الأولى: طريقة القوائم البيضاء.

وهي قوائم تسير على عكس الحكمة التي تقول " المتهم برئ حتى تثبت إدانته " وبعبارة أخرى فكل موقع جديد في شبكة الإنترنت هو موقع محظور ولا يمكن الوصول إليه إلا بعد التأكد تماما من خلوه من الجوانب السلبية ، حينها يمكن إضافته إلى قائمة السماح بالوصول أو القائمة البيضاء. فالأصل هنا هو منع الوصول إلى المواقع.

- الصورة الثانية: طريقة القوائم السوداء.

الأصل في هذا النظام السماح للمستخدمين للوصول لجميع المواقع أي أن " المتهم برئ حتى تثبت إدانته " ويتم المنع فقط عند ثبوت مخالفة الموقع للمعايير المحددة مسبقا.

2- فلترة المعلومات بناء على محتواها:

يتم في هذا النوع اختيار محتوى صفحات الإنترنت لتحديد مدى حفاظها للمعاير المحددة وهناك عدد من الطرق لذلك:

أ. فلترة الكلمات.

يتم هنا فحص الكلمات الموجودة في الصفحات لتحديد ماإذا كانت تحتوي على كلمة تنتمي إلى مجموعة الكلمات الغير لائقة.

وتتميز هذه الطريقة بعدم الحاجة إلى تحديث ومتابعة مستمرة ، ومن عيوبها أنها قد تحجب العديد من المواقع المناسبة ، فمثلا لو حددنا كلمة (تعري) كأحد الكلمات المحظورة فإن المواقع الخاصة بمكافحة والتحذير من العري سوف تحجب أيضا فقط لأنها تحتوي عبارة مثل (مكافحة العري)

ب. تحليل الصور.

يتم في هذا الأسلوب إستخلاص الخصائص العامة للصورة مثل الألوان والنصوص والأشكال ومحاولة تحديد ماإذا كانت تحتوي على صور غير لائقة وهذا النوع يحتاج إلى أجهزة ذات إمكانية عالية للقيام بالعمليات المعقدة الخاصة بتحليل الصور.

خامساً: برامج الحماية:

تقوم برامج الحماية بحماية الأجهزة من تعرضها للفيروسات أو الإختراقات أو التجسس أثناء العمل على شبكة الإنترنت بالفحص الدورى لكل العمليات التى تتم وهذا بفحص البصمات المختلفة التى يتركها الفيروس على البرمجيات أو الملفات مع ضرورة تحديث برامج مكافحة الفيروسات ومتصفح الشبكة أولاً بأول مع ضرورة فصل جهاز الحاسب الآلى عن الشبكة في حالة عدم الإستخدام.

إضافةً لبرامج الحماية يوجد أيضاً الجدار الناري (Firewall) وهو تطبيق برمجي يقوم بمراقبة جميع البيانات والمعطيات، و الهدف الرئيسي من الجدار الناري هو حماية المعطيات المخزنة من أي هجوم يقوم به العابثين والمخترقين، ويمكن إعداد الجدران النارية بحيث تتمكن من مراقبة أنماط معينة من البيانات، كالأوامر والتعليمات ومن الممكن القيام بحجب بيانات من مصادر معينة، كالمعلومات الآتية من دولة معينة، أو من مستخدم معين، إضافةً لحماية البريد الإلكتروني الوارد والصادر.

وهناك عدة أنواع للجدار النارى على النحو التالى[1]:

(أ) **جدران نارية لحماية المنشآت الكبيرة (Enterprise):** وهذا النوع توفره شركات كبرى متخصصة مثل (CISCO) و(Nortel) و(Symantec). وغالباً ما توفر الشركة المصنعة أنواعاً متعددة من جدران الحماية تتفاوت من حيث سرعتها والخدمات التي تقدمها، وهذا النوع من جدران الحماية يتميز بما يلي:

(1) أن جدار الحماية يكون . غالباً . في جهاز قائم بذاته مصمم لغرض معالجة البيانات بسرعة فائقة، أي أنه ليس مجرد برنامج يعمل في جهاز حاسوب عادي.

(2) تعدد الخدمات التي يقدمها جدار الحماية، مثل: غربلة المظاريف، والحماية ضد الفيروسات، وحماية البريد الإليكتروني، والتشفير.

---

(1) د. خالد بن سليمان الغثير ، د. محمد بن عبد الله القحطانى ، أمن المعلومات بلغة ميسرة ، مركز التميز لأمن المعلومات ، جامعة الملك سعود ، الطبعة الأولى ، 2009 ، ص 89 . 92 .

(3) تشغيل جدار الحماية يحتاج إلى مهارات فنية متقدمة.

(4) إرتفاع كلفة الشراء والتشغيل.

(ب) جدران نارية لحماية المنشآت الصغيرة: و هذا النوع يشبه سابقه في كونه جهازا مخصصاً قائماً بذاته، إلا أنه لا يجاريه من حيث سرعة معالجة البيانات أو تعدد الخدمات المقدمة، ولهذا فإنه أقل سعراً.

(ج) جدران نارية لحماية الأجهزة الشخصية: جدران الحماية هذه في أغلبها ما هي إلا برامج تحمل في الحاسوب الشخصي، بحيث تمر من خلالها جميع المعلومات الخارجة من الحاسوب أو الداخلة إليه، وفي هذا المجال أيضا يتنافس عدد من الشركات على السوق الكبير لجدران الحماية الشخصية، ومن أمثلة المنتجات في هذا المجال ما يلي:

(1) Norton Personal Firewall

(2) ZoneAlarm.

(3) Sygate

(4) McAfee

ويقدم هذا النوع من جدران الحماية عدة خدمات مثل غربلة المظاريف، والحماية ضد الفيروسات، وحماية البريد الإليكتروني، والتشفير، والوقاية من برامج التجسس (Spyware)، ويمكن تنزيل هذه البرامج من شبكة الإنترنت، إما مجاناً مثل: (ZoneAlarm)، أو بثمن مثل (ZoneAlarm Pro).

وعندما يحاول برنامج موجود داخل الحاسوب الاتصال بالخارج، كالإتصال بموقع موجود على شبكة الإنترنت، يقوم جدار الحماية (ZoneAlarm) بعرض رسالة كتلك ويطلب من المستخدم إتخاذ القرار بشأن السماح للبرنامج بالإتصال بالخارج أو منعه من ذلك. وبهذه الآلية يمنع جدار الحماية البرامج الخبيثة التي قد توجد في جهاز المستخدم من تسريب المعلومات المخزنة في الجهاز إلى الخارج دون علم المستخدم، كما أن جدار الحماية يمكن تهيئته بحيث يعرض رسالة تحذيرية في كل مرة يحاول برنامج موجود بالخارج الإتصال بالحاسوب الذي يوجد به جدار الحماية، والغرض من هذا واضح، فإنه توجد في شبكة الإنترنت برامج خبيثة كثيرة تحاول الوصول إلى الحواسيب لإتلافها أو إتلاف البيانات التي فيها.

إضافةً لكل ما سبق فإن على مستخدم شبكة الإنترنت أن يحتاط دائماً أثناء وجوده على

شبكة الإنترنت وأن يضع فى حسبانه ما يلى[1]:

. ضرورة تحديث نظام التشغيل المستخدم فى الحاسب الآلى بصفة مستمرة.

. عدم وضع أى بيانات حقيقية أو شخصية أو صور عائلية وحفظها على البريد الإليكترونى.

. عدم إستقبال أى برامج أو ملفات عبر البريد الإليكترونى من أشخاص غير معروفين لأنها يمكن أن تنطوى على ما قد يدمر جهاز الحاسب الآلى أو كشف كل المعلومات التى يحتويها .

. عدم التحدث مع شخص بدون سابق معرفة به لإحتمال قيامه بسرقة البريد الإليكترونى الشخصى.

. عدم الدخول إلى الغرف المشبوهة أو المواقع الإباحية على شبكة الانترنت.

---

(1) راجع موقع وزارة الداخلية المصرية على الإنترنت
http://citizen-service.moiegypt.gov.eg/crimes_web/main.htm

المطلب الثانى

التصدى الشرطى لجرائم الإنترنت

تلعب الشرطة دوراً مهماًً كذلك فى مكافحة جريمة الإنترنت ، ونقصد بالشرطة هنا هم أفراد الشرطة المتخصصين فى مثل هذا النوع من الجرائم والمؤهلين الذين تلقوا تدريباً على إستخدام تقنيات شبكة الإنترنت والقادرين على إستخدام الأجهزة الفنية الحديثة التي تساعد على إثبات الجريمة، ويمكن تسمية الشرطة المتخصصة بجرائم الإنترنت شرطة الإنترنت.

ويقصد بشرطة الإنترنت نوع من الإجراءات والضمانات تقوم بها ضبطية قضائية مختلفة تماماً عن تلك التى تقوم بالكشف عن الجرائم التقليدية ، لكونها لا تعتمد على التدريبات المادية أو الفيزيولوجية التى يتلقاها رجال الشرطة للوصول إلى هذه المرتبة، وإنما تعتمد على قوة تكوين البناء العلمى والتكنولوجى لأفرادها ، وهى تتولى فى ذلك مهمة مباشرة جمع الإستدلالات والتحرى فى العالم الإفتراضى ، من أجل كشف النقاب عن هذا النوع المتميز من الإجرام ، كما يمكنها أن تطارد الهكرة ومخترقى الأنظمة على كافة المستويات(1).

وقد تنبه المجتمع الدولى لخطورة جرائم الإنترنت وما قد يواجه رجال الشرطة من مصاعب تقنية فى إستخلاص وكشف خبايا هذه الجرائم ، وكان ذلك في المؤتمر الثاني للرابطة الدولية للقانون الجنائي الذي عقد في أمستردام بهولندا عام 2000 ونبه المؤتمرون آنذاك إلى ضرورة إعداد رجال قانون لديهم المهارة المعلوماتية التي تمكنهم من التعامل مع الجريمة الرقمية بمهارات رقمية ، وهو ما أكدته ندوة إستكهولم لعلم الإجرام التي ضمت أكثر من ٥٠٠ عالماً وخبيراً ومهنياً في مجال علم الإجرام والعدالة الجنائية والتى نظمتها جامعة إستكهولم السويدية بالتعاون مع جامعة بنسلفانيا الأمريكية، ليطرحوا بحوثًا تكشف حقائق مفادها أن المعاملات الرقمية التي دخلت حياة المجتمعات المعاصرة تفرز كل يوم أنماطًا معقدة من الجرائم الرقمية والقائمة على تقنيات عالية مسرحها الفضاء المفتوح، مما يتطلب معاملة رقمية من حيث منعها وإكتشافها والتحقيق فيها والفصل فيها أمام المحاكم والتعامل مع المدانين فيها(2).

وكما أسلفنا فإن أفراد الشرطة المختصين بجرائم الإنترنت لابد من تلقيهم التدريب الكافى على تقنيات الكمبيوتر والإنترنت ، ويشتمل هذا التدريب على أساسيات هامة ينبغى لرجل

---

(1) نبيلة هبة هروال ، المرجع السابق ، ص100.

(2) اللواء دكتور. محمد الأمين البشرى ، بحث بعنوان تأهيل المحققين فى جرائم الحاسب الآلى وشبكات الإنترنت ، بحث مقدم فى إطار حلقة علمية عقدت بالقاهرة تحت عنوان (الإنترنت والإرهاب) فى الفترة من 15 . 2008/11/19 ، جامعة نايف العربية بالتعاون مع جامعة عين شمس ، ص33.

الشرطة أن الإلمام بها وهى تتلخص فى الآتى:

. الإلمام بأصول التعامل مع الحاسوب بالشكل الذى يضمن إمكانية إجراء عمليات المعاينة والتفتيش والضبط للأجهزة والأنظمة المعلوماتية، وإمتلاك مهارات التعرف على المعلومات ذات القيمة أو التى من الممكن الإستفادة منها فى سير التحقيقات والوصول إلى الجناة.

. أنواع الجرائم والمخاطر والتهديدات ونقاط الضعف الناشئة عن إساءة استخدام الحاسب الآلي أو شبكات المعلومات وخصائصها ، وهو أمر منطقى حيث لا يستطيع رجل الشرطة التعامل مع جريمة يجهل ماهيتها.

وتبرز أهمية الإلمام بطبيعة عمل الشبكات فى كونها ضرورة لتصور كيفية إرتكاب الفعل الإجرامى وكيفية إختراق الشبكات والحواسيب ، وكذلك مدى إمكانية متابعة مصدر الإعتداء على الشبكة والمعوقات الفنية التى تحول دون ذلك[1].

. معرفة الأدوات والأساليب المستخدمة فى إرتكاب جرائم الإنترنت ، وهو أمر غاية فى الأهمية خاصةً لمن يتولون مناقشة الشهود وإستجواب المتهمين فبدونه لن يستطيعوا طرح الأسئلة التى تتصل مباشرة بالفعل الإجرامى وأسلوب إرتكابه كما أنها تساعد المحقق على التواصل مع خبير الحاسوب الجنائى عند شرح الأخير ما توصل إليه من أدلة أو قرائن عن الأساليب المستخدمة فى إرتكاب الجريمة والأدوات التى تساعده على القيام بذلك[2].

. معرفة أهم تقنيات أمن الحاسوب والإنترنت وأدواتها وطريقة عملها، حيث أن إكتساب هذه المهارة وإن كان يبدو فى الظاهر أمراً معقداً بعض الشىء إلا أن الأمر فى حقيقته ليس كذلك حيث أن المطلوب أن يساعد معرفة هذه التقنيات المحقق إستيعابها وربطها بمجريات التحقيق بشكل عام وليس أن يجعله خبيراً فيها[3].

وقد قامت العديد من الدول بتهيئة وتأهيل رجال الشرطة لديها فى هذا المجال ، ومن هذه الدول الولايات المتحدة الأمريكية التى قامت بإنشاء دائرة متخصصة فى هذه الجرائم داخل وحدة التحقيقات الفيدرالية (FBI) ، وكذلك بريطانيا التى سارت على نفس المنوال بتأهيل ضباط الإسكوتلانديارد ، أما فى مصر فقد تم إنشاء ما يسمى بإدارة مكافحة جرائم الحاسبات وشبكات

---

(1) د. حسين بن سعيد الغافرى ، بحث بعنوان التحقيق وجمع الأدلة فى الجرائم المتعلقة بشبكة الإنترنت ، ص 2 ، البحث منشور بالموقع الإليكترونى
http://www.eastlaws.com/Others/ViewMorafaat.aspx?ID=33

(2) د. حسين بن سعيد الغافرى ، بحث بعنوان التحقيق وجمع الأدلة فى الجرائم المتعلقة بشبكة الإنترنت ، مرجع سابق ، ص3.

(3) د. حسين بن سعيد الغافرى ، مرجع سابق ، ص3.

المعلومات بوزارة الداخلية ، وكذلك قيام شرطة سلطنة عمان بإنشاء قسم خاص بالجرائم الإليكترونية، وفى السعودية ووفقاً لنظام مكافحة جرائم المعلوماتية فقد تم إنشاء ما يسمى بشرطة الإنترنت كذلك.

ويبدأ التحقيق الشرطى فى جرائم الإنترنت بإحدى الطرق التالية[1]:

أولاً : تلقى جهة التحقيق معلومات أمنية تشير إلى ممارسة شخص معروف أو غير معروف أنشطة تندرج تحت تعريف جريمة الحاسب الآلى وذلك فى مكان معروف وعلى أجهزة محددة ، ووفق لغات برمجية معلومة.

ثانياً : ضبط شخص وبحيازته أموال مشبوهة أو بطاقات إئتمان مزورة أو بطاقات تعريف مشبوهة.

ثالثاً : بناءً على بلاغ يصل إلى علم جهة التحقيق من متضرر يفيد وقوع تلاعب أو ممارسات خاطئة فى حقه أو حق آخرين ، سواء كان ذلك فى شكل من أشكال عجز مالى فى حسابات مؤسسة مالية أو ضياع حقوق أو تغيرات فى الودائع (دون أن يدرك ما إذا كان ذلك من جرائم الحاسب الآلى أم لا).

رابعاً : توفر معلومات عن نشر فيروسات تخريبية أو رسائل غير مشروعة عبر شبكات الإنترنت.

خامساً : توفر معلومات عن وقوع عمليات إعتراض أو قرصنة فضائية للمعلومات أو تسبيب ضرر بأجهزة ومعدات تعمل بتقنية الحاسب الآلى.

بعد ذلك تبدأ عمليات البحث والتحرى من قبل الشرطة للتأكد من صحة البلاغات أو المعلومات والتقارير التى وردتها.

وتقوم شرطة الإنترنت مثلها مثل الشرطة التقليدية حال وقوع جريمة بعمليات البحث والمعاينة والتفتيش والضبط والإستعانة بشهادة الشهود مع وجود بعض الإختلافات الراجعة إلى الأسلوب التقنى للجريمة وفيما يلى بيان ذلك.

1 - البحث الجنائى:

من الجدير بالذكر أنه فى هذا إطار البحث الجنائى يكتنف عمل شرطة الإنترنت بعض المصاعب التى تتمثل فى :

---

(1) أنظر فى ذلك ، اللواء دكتور. محمد الأمين البشرى ، التحقيق فى الجرائم المستحدثة ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، الطبعة الأولى ، 1425هـ ، ص 108 . 109.

. أن بعض الجرائم التى ترتكب قد تتم خارج الحدود الوطنية للدولة برغم أن نتيجتها قد تحققت على التراب الوطنى ، وهو ما يعكس صعوبة ملاحقة مرتكبى هذه الجرائم الأمر الذى يحتم ضرورة الإلتجاء إلى التعاون الدولى فى هذا المجال.

. أن جريمة الإنترنت لا تخلف أى آثار مادية ملموسة نظراً لإستهدافها البيانات والمعلومات. أضف إلى ذلك غياب الدليل المرئى الممكن بالقراءة فهمه وإفتقاد أكثر الآثار التقليدية ، وسهولة محو الدليل أو تدميره فى زمن قصير جداً ، والضخامة البالغة لكم المعلومات والبيانات المتعين فحصها[1]، فالجرائم التي ترتكب على العمليات الإليكترونية التي تعتمد في موضوعها على التشفير والأكواد السرية والنبضات والأرقام والتخزين الإليكتروني يصعب أن تخلف وراءها آثاراً مرئية قد تكشف عنها أو يستدل من خلالها على الجناة[2].

. والهدف من قيام الجانى بمحو الدليل ، هو عدم تمكين السلطات من كشف جرائمه إذا ما علمت بها، وفي الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم إستطاعة هذه السلطات إقامة الدليل ضده.

. وفى بعض الحالات وبدلاً من أن يقوم الجانى بمحو الدليل المتحصل من الجريمة ، فإن بعض المجرمين المحترفين قد يقومون بوضع تدابير أمنية واقية تزيد من صعوبة كشف سترهم ، وكمثال لذلك نجد أنهم قد يستخدمون تقنيات تمكنهم من إخفاء الأدلة التي قد تكون قائمة ضدهم، وقد يدسون تعليمات خفية بين الأدلة لتصبح كالرمز فلا يمكن لغيرهم أن يفهم مقصودها، وقد يقوم هؤلاء أيضا بتشفير التعليمات بإستخدام طرق وبرامج تشفير البيانات المتطورة مما يجعل الوصول إليها في منتهى الصعوبة[3].

. ومما يصعب الأمور كذلك إمتناع المجني عليهم عن الإخطار بوقوع هذه الجرائم سواءً بقصد حال علمهم بوقوعهم ضحية لفعل إجرامى ما على الشبكة ، كالمؤسسات المالية والبنوك والمؤسسات الإدخارية وشركات الإقراض والسمسرة، حيث يخشى القائمون على إدارتها من شيوع أمر الجرائم التي تقع داخلها على الثقة فيها من العملاء المتعاملين معها، مما قد

---

(1) عبد الرحمن محمد بحر ، معوقات التحقيق فى جرائم الإنترنت، المرجع السابق ، ص47.

(2) د. جميل عبد الباقى الصغير ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت ، المرجع السابق ، ص4.

(3) د. محمد عبد الرحمن سلطان العلماء، جرائم الإنترنت والإحتساب عليها، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت ، كلية الشريعة والقانون ، جامعة الإمارات العربية المتحدة ، 5/3.1 /2000 ، ص7.

يؤدي إلى إنصرافهم عنها[1]، أو بدون قصد فى حالة عدم تفطنهم للجريمة المرتكبة.

وقد أشار تقرير صادر عن الأمم المتحدة عام 1994 إلى أن عدد الحوادث المبلغ عنها قد لا تمثل سوى 5 ٪ من مجموع الجرائم التي ارتكبت[2].

ومما لا شك فيه أن الإحجام عن الإبلاغ عن هذه الجرائم يؤدى فى نهاية الأمر إلى زيادة العدد المرتكب منها.

ولذلك فقد إقترح البعض خاصة في الولايات المتحدة الأمريكية بأن تفرض النصوص المتعلقة بجرائم الحاسبات إلتزاما على عاتق موظفي الجهة المجني عليها بالإبلاغ عن الجرائم التي تحدث داخل هذه الجهة ويتحقق علمهم بها[3].

ويواجه مأمور الضبط مشكلة أخرى فى مجال البحث الجنائى تتمثل فى إنتشار مقاهى الإنترنت التى يستطيع أى فرد من خلالها أن يتعامل مع شبكة الإنترنت بما في ذلك المجرم الذى يستخدمها لإرتكاب جرائمه ، ومرجع تلك الصعوبة هو عدم إلتزام بعض من تلك المقاهى بشروط التراخيص ، بالإضافة إلى إمكانية تنقل ذلك المجرم بين أكثر من مقهى خلال اليوم الواحد ، مما يؤدى إلى صعوبة التوصل بصورة دورية لأدلة الإثبات ، لقيام تلك المقاهى بإعادة تشكيل وتنظيم الأجهزة ، ولاسيما وأن تلك الأدلة توصف بغير المرئية وبأنها سهلة المحو التدميرفى زمن قصير جداً[4].

ولتسهيل عملية البحث فإنه من الضروري تحديد هوية المشتركين بشبكات الإنترنت لتسهيل عمل الشرطة في حال وقوع أي مخالفة، حيث يجب على مقدم الخدمة أن يكون قادراً على تقديم بيانات شخصية عن زبائنه، الأمرالذى يقتضي من هذا الأخير أن يطلب البيانات الشخصية لكل عميل يطلب الإشتراك عبر شبكته.

وكذلك تقع على مقدم الخدمة تجاه الشرطة مسئولية أخرى ألا وهى البيانات التي تتعلق بالإتصالات لكل مستخدم، والتى تتمثل فى المواقع التي ولجها، والمعلومات التي طلبها والبيانات التي حصل عليها فهذه المعلومات وغيرها ذات أهمية كبرى فى عملية البحث

---

(1) د.هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية (دراسة مقارنة) ، مكتبة الآلات الحديثة ، أسيوط ، 1994 ، ص25.

(2) Glenn Wahlert, CRIME IN CYBERSPACE: TRENDS IN COMPUTER CRIME IN AUSTRALIA, Paper presented at the conference: Internet Crime, held in Melbourne, 16-17 February 1998, by the Australian Institute of Criminology,p4.

(3) د.هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية (دراسة مقارنة) ، المرجع السابق ، ص26.

(4) نبيلة هبة هروال ، المرجع السابق ، ص 170.169.

والتحقيق.

وقد نص نظام مكافحة الجرائم المعلوماتية فى السعودية فى مادته الرابعة عشرعلى ذلك حيث نصت المادة المذكورة على أنه (تتولى هيئة الإتصالات وتقنية المعلومات وفقاً لإختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة).

وفى سبيل ذلك ينبغي على المحققين البقاء فى حالة إتصال مع مزودى خدمة الشبكة والزامهم بالإحتفاظ وتجميد السجلات والإتصالات التي قد تكون ذات صلة بالتحقيق، وغيرها من الأدلة التى تساعد فى عملية كشف الحقائق[1].

ومع ذلك فإن الإمكانيات الفنية المتعددة التي تسمح باستخدام الشبكة بطريقة مجهولة أو إمكانية مسح البيانات يثير مصاعب حقيقة بشأن إقامة الأدلة، فالإحتفاظ بالبيانات هو موضوع هام لفعالية التحقيقات.

2 ـ المعاينـــة:

أما بالنسبة للمعاينة التى تعرف بأنها إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها وكذلك جمع الأشياء الأخرى التى تفيد فى كشف الحقيقة[2].

وللمعاينة أهمية كبرى فى الجرائم التقليدية ، حيث يوجد مسرح فعلى للجريمة يحتوى على آثار مادية فعلية ، يهدف القائم بالمعاينة إلى التحفظ عليها تمهيداً لفحصها لبيان مدى صحتها فى الإثبات ، فليس الحال كذلك بالنسبة للجرائم الإليكترونية ، حيث يندر أن يتخلف عن إرتكابها آثار مادية ، وقد تطول الفترة الزمنية بين وقوع الجريمة وإكتشافها ، مما يعرض الآثار الناجمه عنها إلى المحو أو التلف أو العبث بها[3].

والمعاينة قد تكون شخصية إذا تعلقت بشخص المجني عليه ، أو مكانية إذا تعلقت بالمكان الذي تمت فيه الجريمة ، ووضع الشهود والمتهم والمجني عليه ، وقد تكون عينية وهى التي تتعلق بالأشياء أو الأدوات المستخدمة في إرتكاب الجريمة، وفى إطار جرائم الكمبيوتر

---

(1) Daniel A. Morris ,an article entitled, racking a Computer Hacker ،USA Bulletin ، available at http://www.justice.gov/criminal/cybercrime/usamay2001_2.htm

(2) د. مأمون محمد سلامة ، قانون الإجراءات الجنائية معلقاً عليه بالفقه وأحكام النقض ، الطبعة الثانية ، 2005 ، بدون دار نشر ، ص383.

(3) د.هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية (دراسة مقارنة) ، المرجع السابق، ص59.

والإنترنت فإنه لاتوجد أى صعوبة تذكر إذا كانت الجريمة واقعة على المكونات المادية للكمبيوتر، إذ أن الأدلة المادية التى تسمح بتحليل الأمر ونسبة الجريمة إلى شخص معين بالذات متوافرة أما الصعوبات الحقيقية التي تواجه رجال الشرطة فى هذا المجال عندما يكون الفعل الإجرامى قد وقع على برامج الكمبيوتر أو بياناته وبرامجه أو بواسطتها ومرجع ذلك قلة الآثار المادية التي قد تنتج عن هذا النوع من الجرائم وكثرة عدد الأشخاص الذين قد يترددون على مسرح الجريمة خلال المدة الفاصلة بين وقوع الجريمة والكشف عنها.

ويجب على المحقق الذي يقوم بمعاينة الجريمة المعلوماتية يجب أن يكون ملماً بمهارات هذه التقنية ، مثل القدرة على إستخدام برامج Time stamp وهي البرامج التي يمكن عن طريقها تحديد الزمن الذي تم فيه السلوك الاجرامي، لأن ذلك لا يكون متاحاً في جميع الأنظمة المعلوماتية[1].

وللحفاظ على مسرح الجريمة يجب الأخذ فى الإعتبار مايلى[2]:

. تصوير الكمبيوتر وما قد يتصل به من أجهزة بدقة تامة وأخذ صورة لأجزائه الخلفية وسائر ملحقاته.

. ملاحظة طريقة إعداد نظام الكمبيوتر بعناية بالغة.

. إثبات الحالة التي تكون عليها توصيلات وكابلات الكمبيوتر والمتصلة بمكونات النظام.

. عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة خشية إتلاف البيانات المخزنة.

3 - التفتيش:

أما التفتيش والذى يعرف بأنه البحث عن شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها[3] ، فإنه فى مجال جريمة الإنترنت ينصب على إستخراج المعلومات التي من شأنها أن تساعد التحقيق كتفتيش بنوك المعلومات وفحص كل الوثائق المحفوظة ومراسلات مرتكب الجريمة مثل الرسائل الإلكترونية وفك شفرات الرسائل المشفرة.

---

(1) أ.رحاب عميش ، الجريمة المعلوماتية ، بحث مقدم إلى المؤتمر المغاربي الأول حول (المعلوماتية والقانون) ، المنعقد في الفترة من 28 . 29 أكتوبر 2009 ، أكاديمية الدراسات العليا ، طرابلس ، ليبيا ، ص31.

(2) القاضى . وليد عالكوم ، بحث بعنوان التحقيق فى جرائم الحاسوب ، ص6 ، البحث منشور بالموقع الإليكترونى : http://www.4shared.com/file/WLlIhQTH/_.html

(3) د.عوض محمد عوض ، المبادئ العامة في قانون الإجراءات الجنائية ، دار المطبوعات الجامعية ، 1999 ، ص377.

ويشترط فى التفتيش الحاصل بسبب جرائم الإنترنت:

1. أن تكون هناك جريمة وقعت على البيانات والمعلومات المخزنة بالكمبيوتر أو بإساءة إستخدام الكمبيوتر كأداة في إرتكاب جرائم عبر الإنترنت وشبكات المعلومات.

2 . ويشترط كذلك فى هذا التفتيش وجود إتهام موجه إلى شخص بإرتكاب الجريمة بناءً على دلائل قوية تدعو للإعتقاد بإرتكابه للجريمة التي وقعت ، وإن كان الأمر لا يعد مشكل بالنسبة للضابط فى الجرائم التقليدية فإن الأمر ليس بهذه السهولة في نطاق جرائم الكمبيوتر والإنترنت، فالعثور على هذه الأدلة أو القرائن يحتاج إلى إستخدام تقنيات التكنولوجيا الحديثة.

3 . أن تكون هناك دلائل أو قرائن على وجود ما يفيد في كشف الحقيقة فالتفتيش يهدف إلى غاية معينة وهي الحصول على أشياء تتصل بالجريمة المرتكبة وتفيد في كشفها، وبالتالى فإن التفتيش لا يقع إلا على الأجهزة والمعدات التى تكون هناك دلالات وأمارات على فائدتها فى كشف حقيقة الأمور.

4 . يخضع التفتيش للخصائص العامة التي تخضع لها كافة إجراءات التحقيق الابتدائي، وهي وجوب التدويين بمعرفة كاتب والسرية عن الجمهور وحضور الخصوم ووكلائهم كلما أمكن ذلك، كذلك لابد أن يكون أمر التفتيش مسبباً.

5 . ومحل التفتيش فى جريمة الإنترنت هو مكونات جهاز الكمبيوتر سواء كانت مادية أو معنوية أو شبكات الإتصال الخاصة به بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش.

وإن كان ليس ثمة خلاف على تفتيش المكونات المادية للحاسب الآلى ، إلا أن التفتيش الحاصل على المعلومات والبيانات المعالجة إليكترونياً ، يثير جدلاً واسعاً يتمثل فى صلاحيتها لأن تكون موضوعاً للتفتيش والضبط من عدمها(1).

فثمة إتجاه يرى أن هذه المكوّنات المنطقية لا تصلح بطبيعتها لأن تكون محلاً للتفتيش، على إعتبار أن التفتيش يهدف في المقام الأول إلى ضبط أدلة مادية ، وهذا يستلزم وجود أحكام

---

(1) راجع فى ذلك أسامة المناعسة ، أ. جلال محمد الزعبي ، أ. صايل فاضل الهواوشة ، جرائم الحاسب الآلي والإنترنت ، مرجع سابق ، ص278 وما بعدها.

خاصة تكون أكثر ملاءمة لهذه البيانات اللامحسوسة[1].

وفي المقابل ، إنبرى إتجاه آخر مؤدّاه أن المكونات المعنوية لا تختلف عن الكيان المادي للحاسب الآلي من حيث خضوعها لأحكام التفتيش وما في حكمه ، بدعوى أن البيانات ، التي هي عبارة عن نبضات إلكترونية ، قابلة للتخزين على أوعية أو وسائط مادية كالأشرطة الممغنطة والأقراص والأسطوانات ، كذلك يمكن تقديرها وقياسها بوحدات قياس خاصة معروفة ، وعلى هذا الأساس تكون صالحة كموضوع للضبط والتفتيش شأنها شأن الوسائط المادية ذاتها[2].

ووفقاً لما نظنه صحيحاً ، فإن الاتجاه الثانى أكثرقبولاً ومنطقية ، فالقول بغير ذلك معناه إطلاق يد الجناة للعبث بأنظمة الحاسب الآلى وشبكات الكمبيوتر بحجة أن ما سيحدث صعب ضبطه وتفتيشه ، فبالرغم من أن البيانات المعالجة تتطلب قواعد خاصة تحكمها بدلاً من محاولة تطويع القواعد التقليدية وتوسيع نطاقها ، إلا أنه يجب العمل بالقواعد التقليدية ولومؤقتاً إلى حين وضع تصور شامل للجريمة وكيفية إرتكابها ومدى إمكانية تطبيق الإجراءات بشأنها فهذه كلها صعوبات مرجعها حداثة هذا النمط من الجرائم وعدم تمرس جهات التحقيق على التعامل معها.

ولعله من الصحيح وفى سبيل مواجهة هذا القصور إمكانية إضافة نصوص إلى قانون الإجراءات الجنائية فيما يتعلق بالتفتيش الواقع على نظم المعلومات ليشمل التفتيش إضافة للأدلة المادية الأدلة المعنوية التى تتعلق ببيانات الحاسب الآلى.

وبإستقراء موقف التشريعات الحديثة نجدها قد ذهبت إلى تأكيد هذا الإتجاه ، بحيث أضحت المكونات المعنوية للحاسب الآلي ضمن الأشياء التي تصلح أن تكون محلاً للتفتيش والضبط . ففي التشريع الأمريكي على سبيل المثال تقضي المادة (34) من القواعد الفيدرالية الخاصة بالإجراءات الجنائية الصادرة سنة 1970 بعد تعديلها بمد نطاق التفتيش ليشمل ضمن ما يشمل أجهزة الحاسب الآلي وأوعية التخزين والبريد الإلكتروني والصوتي والمنقول عن طريق الفاكس[3].

وكذلك المادة 251 من قانون الإجراءات الجنائية اليونانى التى تعطي سلطات التحقيق

---

(1) د. موسى مسعود أرحومة ، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية ، بحث مقدم إلى المؤتمر المغاربي الأول حول (المعلوماتية والقانون) ، المنعقد في الفترة من 29.28 أكتوبر 2009 ، أكاديمية الدراسات العليا ، طرابلس ، ليبيا ، ص8.

(2) د. موسى مسعود أرحومة ، المرجع السابق، ص9.

(3) د. موسى مسعود أرحومة ، المرجع السابق، ص9.

إمكانية القيام بأي شيء يكون ضروريا لجمع وحماية الدليل.

وكذلك المادة 487 من قانون العقوبات الكندى التى تقضى بإمكانية إصدار أمر قضائى لتفتيش وضبط أى شىء ... تتوافر بشأنه أسس ومبررات معقولة تدعو للإعتقاد بأن جريمة قد وقعت أو يشتبه فى وقوعها ، أو أن هناك نية لإستخدامه فى إرتكاب جريمة ، أو أنه سينتج دليلاً على وقوع جريمة[1].

- **مدى خضوع شبكات الحاسب للتفتيش:**

قد يكون حاسب المتهم متصلاً بغيره من الحواسيب عبر شبكة ، وهنا ينبغي التمييز بين ما إذا كان حاسوب المتهم متصلاً بآخر داخل إقليم الدولة أو كان متصلاً بحاسوب يقع في نطاق إقليم دولة أخرى .

أ ـ في حالة ما يكون حاسوب المتهم متصلاً بجهاز آخر داخل إقليم الدولة :

بالرجوع إلى القواعد العامة للتفتيش في قانون الإجراءات الجنائية فإن جهاز الحاسوب إذا كان موجوداً بمنزل غير المتهم فلا يجوز تفتيشه من قِبل جهة التحقيق إلاّ بعد استصدار إذن من القاضي الجزئي قبل تفتيشه ، وإلاّ كان الإجراء باطلاً غير أن صدور الإذن قد يستغرق بعض الوقت ، ما قد يؤدي إلى تلاشي الدليل واندثاره ، وهذا ربما يعيق الوصول إلى دليل يساعد فى فك طلاسم الجريمة.

ويبرز هنا تساؤل هام حول إمكانية قيام المحقق بالتفتيش فى هذه الحالة من عدمه ، فمثلاً قانون تحقيق الجنايات البلجيكي الصادر في 23 نوفمبر 2000 ، يجيز إمتداد التفتيش إلى نظام معلوماتي آخر غير مكان البحث الأصلي ، ولكن ليس بصورة مطلقة وإنما بقيود معينة ، يمكن إجمالها في أن تكون ثمة ضرورة لكشف الحقيقة فيما يخص الجريمة موضوع البحث أو أن تكون الأدلة معرضة لمخاطر معينة كالإتلاف أو التدمير وما شابه[2].

وكذلك نص مشروع قانون جريمة الحاسب فى هولندا على إمكانية أن يمتد التفتيش إلى الأجهزة المعلوماتية الموجودة فى موقع آخر شريطة أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة وذلك شريطة الضرورة وأن يكون التدخل مؤقتاً[3]. وهو ما نصت عليه كذلك المادة 19 من إتفاقية بودابست لجرائم الإنترنت.

---

(1) د. هلالى عبد اللاه أحمد ، تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى ، دراسة مقارنة ، دار النهضة العربية ، 2006 ، ص201.

(2) د. موسى مسعود أرحومة ، المرجع السابق، ص12.

(3) د. طارق إبراهيم الدسوقى عطية ، المرجع السابق ، ص387.

ب ـ في حالة اتصال حاسوب المتهم بآخر موجود بإقليم دولة أخرى :

بغية إعاقة الوصول إلى الدليل قد يعمد الجناة إلى تخزين البيانات غير المشروعة في حاسوب خارج إقليم الدولة.

وعلى الرغم من إمكانية القيام بالبحث وإقامة الأدلة وضبط الأدوات التي تقع خارج النطاق المحلي إلا أن ذلك يصطدم بمبدأ إحترام سيادة الدول، فعندما تكون البيانات مخزنة لدى مؤدي خدمة أجنبي فإنه بالرغم من إمكانية تفتيشها من الناحية الفنية داخل النطاق الإقليمي، إلا أنه لا بد من موافقة سلطات البلد المعني ووفقاً للإجراءات المعقدة للتعاون القضائي، وفي كل الأحوال يبدو أن الدول غير مستعدة اليوم لقبول طلبات إجراء التفتيش الإلكتروني العابر للحدود التي تعتبرها بمثابة مساس بسيادتها[1].

وفى هذه الحالة فإن إمتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافى للدولة التى صدر من جهاتها المختصة الإذن ودخوله فى المجال الجغرافى للدولة الأخرى وهو ما يسمى بالولوج عبر الحدود قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها ، لذا فإن جانب من الفقه يرى بأن التفتيش الإليكترونى العابر للحدود لابد وأن يتم فى إطار إتفاقيات خاصة ثنائية أو دولية تجيز هذا الإمتداد تعقد بين الدول المعنية ، وبالتالى فإنه لا يجوز القيام بذلك التفتيش العابر للحدود فى غياب تلك الإتفاقيات أو على الأقل الحصول على إذن الدولة الأخرى ، وهو ما يؤكد على ضرورة التعاون الدولى فى مجال مكافحة الجرائم التى تقع فى المجال الإليكترونى[2].

ولأجل مواجهة هذه المشكلة في نظر الفقه المقارن (الهولندي على سبيل المثال) ينبغي إلتماس طلب من سلطات الدولة الأخرى بنسخ البيانات المخزنة في الحواسيب الموجودة على أراضيها وإرسالها إلى الدولة الطالبة . غير أن هذا الأسلوب . المعروف بأسلوب التفويض والالتماس . يُعاب عليه أنه يفتقر إلى الفعالية نتيجة الإجراءات الروتينية التي تفضي إلى تأخير الوصول إلى الدليل وربما ضياعه أو إتلافه[3].

والإتجاه الرافض لإمتداد التفتيش إلى الحواسيب الأخرى لا يقر هذا الإجراء إلاّ بموجب

---

(1) د. صالح أحمد البربري ، بحث بعنوان ، دور الشرطة في مكافحة جرائم الإنترنت في إطار الإتفاقية الأوروبية ، ص9، منشور بالموقع الإليكترونى :
http://lawjo.net/vb/showthread.php?p=6024

(2) راجع فى ذلك د. محمد أبو العلا عقيدة ، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية ، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، أكاديمية شرطة دبي ، مركز البحوث والدراسات ، 26-4/28/ 2003 ، دبي – الإمارات العربية المتحدة ، ص10.

(3) د. موسى مسعود أرحومة ، المرجع السابق، ص13.

اتفاقية دولية ، وهو يعبر عن الرأي السائد في الفقه الألماني .

وسيراً في هذا الإتجاه ، عرضت على القضاء الألماني واقعة تتعلق بالغش المعلوماتي ، حيث كانت طرفية الحاسب الموجودة بألمانيا متصلة بأخرى بسويسرا . وبالرغم من أن السلطات الألمانية (سلطات التحقيق) قد حاولت إسترجاع البيانات المخزنة بالخارج ، إلاّ أنها لم تتمكن من ذلك إلاّ من خلال التماس المساعدة المتبادلة[1].

وقد ساور الإعتقاد الشرطة اليابانية بأن مجموعة من المخربين قد إستخدمت أجهزة كمبيوتر في الصين والولايات المتحدة في مهاجمة العديد من المواقع الخاصة للحكومة اليابانية على الشبكة وقد طالبت الشرطة اليابانية كل من بكين وواشنطن بتسليم بيانات الدخول المسجلة على أجهزة الكمبيوتر في كل من هاتين الدولتين حتى تتمكن من الوصول إلى جذور هذه العملية[2].

وفي المقابل ، يؤيد جانب آخر من الفقه أمر إمتداد التفتيش إلى الحواسيب الموجودة خارج إقليم الدولة ، وهذا الرأي يقوم على أساس واقعي ، إذ إن معتنقيه والمدافعين عنه يحاولون التعامل بواقعية مع ما يعترض سلطات التحقيق من مشكلات . وهذا ما يسمح به قانون التحقيق البلجيكي (مادة 88) التى تجيز لقاضي التحقيق الحصول على نسخة من البيانات التي هو في حاجة إليها دونما إنتظار إذن من سلطات الدولة الأخرى[3].

أما إتفاقية بودابست فقد أجازت التفتيش الذى يقتضى الدخول على شبكة معلومات تابعة لدولة أخرى وذلك فى المادة (32) التى نصت على إمكانية الدخول بغرض التفتيش والضبط فى أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها ، وذلك فى حالتين:

أ . إذا كان هذا الإجراء يتعلق بمعلومات أو بيانات مباحة للجمهور.

ب . في حالة الحصول على رضا صاحب أو حائز البيانات بالتفتيش.

4 ـ الضبـــط:

أما الضبط فهو أن يضع مأمور الضبط القضائى يده على شىء يتصل بالجريمة ويفيد فى كشف حقيقتها، ويجب أن تكون الأدلة المأخوذة من الكمبيوتر لها نفس سمات الأدلة التقليدية، وبمعنى أخر يجب أن تكون مقبولة وسليمة ودقيقة، وكاملة ولكن تلك الأدلة لها أيضا سمات محددة

---

(1) راجع فى ذلك ، د. طارق إبراهيم الدسوقى عطية ، المرجع السابق ، ص389.

(2) الرائد الدكتور. عبد الله حسين علي محمود ، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات ، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، أكاديمية شرطة دبي ، مركز البحوث والدراسات ، 26ـ2003/4/28 ، دبي– الإمارات العربية المتحدة ، ص10.

(3) د. موسى مسعود أرحومة ، المرجع السابق، ص13ـ 14.

تخلق مصاعب تواجه من يرغبون في الإعتماد عليها فهي غير مستقرة ويسهل تغييرها دون أن يترك ذلك أثر واضح كما أنها مبتكرة للغاية مما يشكل عائق أمام جهات التحقيق.

والضبط فى جرائم الإنترنت قد يقع على أدلة مادية ملموسة وقد يقع على أدلة معنوية أو رقمية داخل الحاسب الآلى وذلك على النحو التالى :

فالأدلة المادية التي يجوز ضبطها في الجريمة المعلومايتة والتي لها قيمة خاصة في إثبات جرائم الحاسب الآلي ونسبتها إلى المتهم هي(1):

1. **الـورق** : كثير من الجرائم الواقعة على المال أو على جسم الإنسان تترك خلفها قدرا كبيراً من الأوراق والمستندات الرسمية منها والخاصة، إلا أن وجود أجهزة الحاسب يجعل كثيرا من المعلومات يتم حفظها في الحاسب الآلي، مما قلل حجم الأوراق والملفات ومع ذلك نجد أن الكثيرين يقومون بطباعة المعلومات لأغراض المراجعة أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات موضوع الجريمة وأجهزة الحاسب الآلي والطابعات المتطورة ذات السرعة الفائقة تطبق قدرا كبيرا من الأوراق في وقت قصير عليه يعتبر الورق من الأدلة التي ينبغي الإهتمام بها في البحث وتفتيش مسرح الجريمة والورق أربعة أنواع:

   أ – أوراق تحضيرية يتم إعدادها بخط اليد كمسودة أو تصور للعملية التي يتم برمجتها.

   ب– أوراق تالفة تتم طباعتها للتأكد ومن ثم إلقاؤها في سلة المهملات.

   ج– أوراق أصلية تتم طباعتها والإحتفاظ بها كمرجع أو لأغراض تنفيذ الجريمة.

   د– أوراق أساسية وقانونية محفوظة في الملفات العادية أو دفاتر الحسابات وتكون لها علاقة بالجريمة خاصة عند تلقيها أو تزوير بياناتها لتنفيذ جريمة الحاسب الآلي.

2. **جهاز الحاسب الآلي وملحقاته:** وجود جهاز حاسب آلي مهم للقول بأن هناك جريمة ولأجهزة الحاسب الآلي أشكال وأحجام وألوان مختلفة وخبير الحاسب الآلي يستطيع أن يتعرف على الحاسب الآلي ومواصفاته بسرعة فائقة، كما يستطيع تمييزه عن الأجهزة الإلكترونية الأخرى وتحديد أسلوب التعامل معه في حالة الضبط والتحريز.

3. **أقراص الليزر** : مع جهاز الحاسب الآلي الشخصي قد تجد قدراً كبيراً من أقراص الليزر علاوة على أن مراكز الحاسب الآلي في الشركات والبنوك قد تجد فيها الآلاف من الأقراص قد تكون على غلاف القرص بيانات توضح محتويات كل قرص وبمعرفة خبير يقدم الدليل أمام المحكمة وقد تجد في مكان ما أقراص الليزر ولا تجد معها أجهزة حاسب

(1) راجع فى ذلك ، اللواء دكتور. محمد الأمين البشرى ، المرجع السابق، ص 117 . 119.

آلي ومع ذلك يعد جزءاً من جريمة حاسب آلي متى كانت محتوياتها عنصرا من عناصر الجريمة.

4 . **المـودم** : والمودم هي الوسيلة التي تمكن أجهزة الحاسب الآلي من الإتصال مع بعضها البعض عبر شبكة الإنترنت بإستخدام خطوط الهاتف لتبادل البيانات والمعلومات.

5 . **الشرائط الممغنطة** : وتستعمل الشرائط الممغنطة عادة لحفظ نسخ إحتياطية من مكونات جهاز الحاسب الآلى وقد تكون في مكان بعيد آمن.

6 . **الطابعات** : وللطابعات أنواع منها العادية ومنها طابعات ليزرية منها الملونة ومنها غير الملونة.

7 . **البطاقات الممغنطة وبطاقات الإئتمان القديمة والمواد البلاستيكية** : المستعملة في إعداد تلك البطاقات تعتبر قرائن للإثبات في جرائم الحاسب الآلي.

أما الأدلة الرقمية فتعرف بأنها معلومات يقبلها المنطق والعقل ويعتمدها العلم ، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسوب وملحقاتها وشبكات الإتصال ، ويمكن إستخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جاني أو مجني عليه[1].

وتمر عملية تجميع الأدلة الرقمية التي تتم عبر الشبكه بثلاث مراحل هى[2]:

- **المرحلة الأولى** : تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة حيث يتم تقفى أثر الحاسبات التي دخل المجرم منها ومحاولة إيجاد أي أثر له.
- **المرحلة الثانية :** مرحلة المراقبة. وتتم المراقبة بعدة طرق أبرزها:

. إستخدام برامج مراقبة للبحث عن المعلومات المشتبه فيها حصر و تسجيل بيانات كل دخول وخروج بالموقع.

. إستخدام ما يعرف بالحشرات أو Bugs وهي أجزاء توضع في الحاسب الآلي لمراقبته.

. إستخدام كاميرات مراقبة لشاشة الحاسب الآلي معدة للإستخدام التجاري.

(1) اللواء دكتور. محمد الأمين البشرى ، بحث بعنوان تأهيل المحققين فى جرائم الحاسب الآلى وشبكات الإنترنت ، المرجع السابق ، ص25.

(2) Orin S. Kerr , Digital evidence and the new criminal procedure, 2005, P285, available at, http://www.jstor.org/pss/4099310

- **المرحلة الثالثة :** ضبط الأجهزة المشتبه فيها وفحصها.

وبعد إتمام عملية الضبط فإنه من الضروري توثيق الأدلة الرقمية بعدة طرق كالتصوير الفوتوغرافي ، التصوير بالفيديو ، وطباعة نسخ من الملفات المخزنة في جهاز الحاسوب أو المحفوظة في الأقراص ، وعند حفظ الأدلة الرقمية على الأقراص والشرائط يجب تدوين التاريخ والوقت الذى تم فيه الإجراء ، وتوقيع الشخص الذي قام بإعداد النسخة ، و المعلومات المضمنة في الملف المحفوظ(1).

ويواجه عملية الضبط للبيانات المعالجة إلكترونيا صعوبات منها على سبيل المثال(2):

. الحجم الكبير للشبكة التي تحتوي على المعلومات المعالجة إلكترونيا والمطلوب ضبطها.

. وجود هذه البيانات فى شبكات أو أجهزة تابعة لدولة أجنبية مما يستدعى تعاونها مع جهات الشرطة والتحقيق في عملية التفتيش والضبط والتحفظ.

. يمثل التفتيش والضبط أحياناً إعتداءً على حقوق الغير ، أو على حرمة حياته الخاصة فيجب إتخاذ الضمانات اللازمة لحماية هذه الحقوق والحريات.

5 - الخـــبرة.

المحقق الذي يقوم بمعاينة الجريمة المعلوماتية يجب أن يكون ملماً بمهارات هذه التقنية ، مثل القدرة على إستخدام البرامج التي يمكن عن طريقها تحديد الزمن الذي تم فيه السلوك الاجرامي، كذلك يجب أن يكون ملماً بمهارات تحليل البيانات و مهارات التشفير التي تتيح له فك الرموز واستعادة البيانات الملغية .

إضافة لما سبق فإنه من الممكن لمأمور الضبط أن يستفيد كذلك من أعمال الخبرة فى مجال التحقيق فى جرائم المعلوماتية ، وذلك بأن يستعين بالمتخصصين فى علوم الحاسب الآلى والتكنولوجيا لتسهيل ما قد يصعب عليه فى عمليات البحث والتفتيش والضبط والمعاينة ، وجدير بالذكر أن أعمال الخبرة المأمول الحصول عليها قد تقدمها بعض المؤسسات المتخصصة(3).

إضافةً لذلك فقد شرعت بعض الدول في إعداد أجهزة متخصصة للخبرة في الإجرام عبر الإنترنت. وعلى رأس تلك الدول الولايات المتحدة التي قامت بإنشاء وحدة تابعة للمباحث

(1) اللواء دكتور. محمد الأمين البشرى ، بحث بعنوان تأهيل المحققين فى جرائم الحاسب الآلى وشبكات الإنترنت ، المرجع السابق ، ص29. 30.

(2) د. محمد أبو العلا عقيدة ، المرجع السابق ، ص12.

(3) من ذلك قسم دراسات الحاسب الآلي في جامعة ستانفورد ، ومعهد التكنولوجيا في ماساشوستس وغير ذلك من مراكز علوم الحاسب الآلى المتخصصة.

الفيدرالية الأمريكية FBI أطلق عليها المعمل الإقليمي الشرعي للحاسوب ، ومقره سان دييجو San Diego، والذي تم إفتتاحه في نوفمبر 2000 كمركز خبرة عام متعدد النواحي القضائية غرضه مكافحة الجريمة عبر الانترنت ، حيث يتم إعداد محللين شرعيين للحاسب الآلي والذين يعملون بدورهم على تكثيف مواجهة الجريمة عبر الإنترنت.

وبالنسبة لأبرز المسائل التى تحتاج للإستعانة بالخبير فى جرائم الإنترنت فهى كالآتى[1]:

. تركيب الكمبيوتر و طرازه و نوعه و نظام تشغيله و الأنظمة الفرعية التي يستخدمها.

. بيئة الكمبيوتر أو الشبكة من حيث طبيعتها، تركيزها أو توزيعها و كذلك نمط و وسائل الإتصالات.

. المكان المحتمل لأدلة الإثبات و شكلها و هيئتها.

. الآثار الإقتصادية و المالية المترتبة على التحقيق في الجريمة المعلوماتية.

. كيفية عزل النظام المعلوماتي عند الحاجة دون إتلاف الأدلة أو الأجهزة أو تدميرها.

. إمكانية نقل أدلة الإثبات إلى أوعية أخرى دون إتلافها.

. إمكانية نقل أدلة الإثبات إلى أوعية مادية كالأوراق على أن تكون مطابقة لما هو مسجل في الحاسب الآلي أو النظام أو الشبكة.

6 ـ الشهاده:

الشهادة هى الأقوال التى يدلى بها غير الخصوم أمام سلطة التحقيق أو القضاء بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف إرتكابها وإسنادها إلى المتهم أو برائته منها[2].

وفى مجال جرائم الإنترنت والحاسب الآلى فإن الشاهد هو الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي والذي تكون لديه معلومات جوهرية أو هامة لازمة للولوج في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة

---

(1) راجع فى نفس المعنى ، د.هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية (دراسة مقارنة) ، المرجع السابق ،ص142.

(2) د. إبراهيم الغماز ، الشهادة كدليل إثبات فى المواد الجنائية ، رسالة دكتوراه ، كلية الحقوق ، جامعة القاهرة ، 1980 ، ص30.

داخله[1].

والشاهد فى مجال جرائم المعلوماتية ينقسم إلى عدة نماذج كالتالى:

أ ـ القائم على تشغيل الحاسب الآلي.

وهو المسؤول عن تشغيل جهاز الحاسب الآلي والمعدات المتصلة به ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز وإستخدام لوحة المفاتيح في إدخال البيانات كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج[2].

ب ـ المبرمجون.

المبرمج هو الشخص الذي يقوم ببرمجة الحاسوب ويطور برمجيات له. ويمكن إعتباره مهندس برمجيات أومطور برمجيات.

والمبرمجون يمكن تقسيمهم إلى فئتين:

. **الفئة الأولى** : هم مخططو برامج التطبيقات.

. **الفئة الثانية** : هم مخططو برامج النظم.

حيث يقوم مخططوا برامج التطبيقات بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم ثم يقوم بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات، أما مخططو برامج النظم فيقومون بإختبار وتعديل وتصحيح برامج نظام الحاسب الداخلية أي أنه يقوم بالوظائف الخاصة بتجهيز الحاسب بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والإخراج ووسائط التخزين بالإضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج[3].

جـ ـ المحللون.

المحلل وهو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين، ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة وأستنتاج العلاقات الوظيفية من هذه الوحدات، كما يقوم بتتبع البيانات داخل النظام عن طريق ما سمى بمخطط تدفق البيانات واستنتاج

---

(1) د. هلالى عبد اللاه أحمد ، إلتزام الشاهد بالإعلام فى الجريمة المعلوماتية ، دراسة مقارنة ، دار النهضة العربية ، 2006 ، ص23.

(2) د. محمد فهمي ، الموسوعة الشاملة لمصطلحات الحاسب الإليكتروني ، مطابع المكتب المصري الحديث ، 1991 ، ص23.

(3) الرائد الدكتور عبد الله حسين علي محمود ، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات ، المرجع السابق ، ص 15 . 16.

الأماكن التي يمكن ميكنتها بواسطة الحاسب[1].

د ـ مهندسو الصيانة.

وهم المسؤولون عن أعمال الصيانة الخاصة بالحاسب الآلى.

هـ ـ مديرو النظم.

وهم الذين يقومون بأعمال إدارية في النظم المعلوماتية.

وإضافةً إلى الفئات السابقة يحصر قانون الدليل الخاص بولاية كاليفورنيا شهود الجريمة المعلوماتية في[2]:

. أمناء مكتبة الأشرطة الذين يتحملون مسؤولية توفير الأشرطة أو الأسطوانات التي تشتمل على البيانات المصدرية الصحيحة.

. موظفو المدخلات والمخرجات والمسؤولون عن معالجة المدخلات المستخدم في تنفيذ برامجه.

. المستخدم النهائي الذي يمد بالمعلومات المدخلة ويصرح بتنفيذ برامج الكمبيوتر ويستخدم نواتجها.

- **إلتزامات الشاهد المعلوماتي.**

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات بحثاً عن أدلة الجريمة ، وثمة تساؤل يطرح نفسه هل من المفترض قيام الشاهد بطبع الملفات والإفصاح عن كلمات المرور والشفرات؟

وفى سبيل الإجابة على هذا التساؤل ثمة إتجاهان:

- **الإتجـــاه الأول :**

يرى هذا الإتجاه أنه ليس من واجب الشاهد وفقا للإلتزامات التقليدية للشهادة أن يقوم بطباعة البيانات المخزنة فى ذاكرة الحاسوب أو تحليل ذاكرة النظام المعلوماتى ليكشف له عن آثار بعض البيانات[3].

ويميل إلى هذا الإتجاه الفقه الألماني حيث يرى عدم إلتزام الشاهد بطبع البيانات المخزنة

---

(1) د. هلالى عبد اللاه أحمد ، إلتزام الشاهد بالإعلام فى الجريمة المعلوماتية ، المرجع السابق ، ص24.

(2) الرائد الدكتور عبد الله حسين علي محمود ، المرجع السابق ، ص 16.

(3) د.جميل عبد الباقى الصغير ، أدلة الإثبات الجنائى والتكنولوجيا الحديثة ، دراسة مقارنة ، دار النهضة العربية ، 2002 ، ص106.

في ذاكرة الحاسب على أساس أن الإلتزام بأداء الشهادة لا يتضمن هذا الواجب[1].

- **الإتجــاه الثانى :**

ويرى أنصار هذا الإتجاه أن من واجب الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة.

ولعله من المنطق القول أنه مادام من واجب الشاهد تقديم كل مايحوزه من معلومات لجهة التحقيق بحثاً عن أدلة ، فبالتالى يجب عليه الإلتزام بكل مايلزم لخدمة التحقيق حتى ولو إنطوى الأمر على طبع ملفات البيانات أو الإفصاح عن كلمات المرور.

تنظيم إتفاقية بودابست للعمل الشرطى فى مواجهة جرائم الإنترنت:

نظمت الإتفاقية الأوروبية لمكافحة جرائم الإنترنت الموقعة فى بودابست العاصمة المجرية العمل الشرطى فى مواجهة جرائم الإنترنت وذلك فى عدة مواد ، فنصت المادة 14 على:

أ . ضرورة إعتماد كل دولة طرف فى الإتفاقية ما يلزم من تدابير تشريعية وتدابير أخرى لإقرار الصلاحيات والإجراءات لأغراض التحقيق الجنائى.

ب . وفيما عدا ما ورد في المادة 21، يقوم كل طرف بتطبيق السلطات والإجراءات الواردة في الفقرة الأولى على :

. الجرائم التي تقع وفقاً لما هو وارد في المواد من 2–11 من هذه الاتفاقية.

. على كافة الجرائم الأخرى التي ترتكب بإستخدام شبكة المعلومات، وجمع الأدلة الإلكترونية عن كل الجرائم الجنائية.

ونصت المادة 16 على أن لكل دولة طرف أن تتخذ الإجراءات القانونية اللازمة وغيرها لكي تسمح للسلطات المختصة أن تأمر وأن تقتضي بأي طريق سرعة حفظ المعلومات الإلكترونية الخاصة والمخزنة بواسطة شبكة المعلومات وعلى الأخص عندما يوجد سبب يدعو للإعتقاد أن تلك المعلومات عرضة للفقد أو التعديل.

ونصت المادة 18 على أنه على كل دولة طرف إتخاذ الإجراءات التشريعية اللازمة لمنح السلطات المختصة بإصدار الأمر إلى :

. أي شخص يتواجد داخل حدود الدولة أن يعطي البيانات المعلوماتية الخاصة، التي يملكها أو

(1) Mohrenschloager (Manfred): Computer crimes and other crimes against information technology in Germany "R.I.D.P 1993 P. 351.

التي تقع تحت سلطته، والمخزنة في إحدى شبكات المعلومات أو أي مستودع لتخزين المعلومات.

. أي مؤدي خدمة يقوم بتقديم مثل هذه الخدمات داخل الدولة أن يبلغ عن البيانات التي في حوزته أو تحت إشرافه المتعلقة بالمشتركين والخاصة بمثل هذه الخدمة.

ويقصد ببيانات المشتركين فى هذه المادة أية معلومات فى صورة بيانات كمبيوتر أو أى صورة أخرى يتم حفظها من جانب مقدم الخدمة وهذه المعلومات يمكن التوصل بموجبها إلى :

. نوع خدمة الإتصال المستخدم والأدوات الفنية المستخدمة في هذا الصدد ومدة الخدمة.

. هوية المشترك ، وعنوانه البريدي أو الجغرافي ورقم تليفونه أو أي رقم اتصال آخر، والبيانات المتعلقة بالفواتير والدفع الموجودة بموجب عقد الإتفاق على الخدمة.

. أي معلومات أخرى تتعلق بمكان وجود معدات الإتصال والموجودة بناء على إتفاق لتأدية الخدمة.

ونصت المادة 19 على أن:

1. لكل طرف إتخاذ الإجراءات التشريعية لكي يمنح السلطات المختصة إذناً بالتفتيش أو الدخول بطريقة مشابهة على :

أ – أي شبكة معلومات أو لجزء منها، وكذلك البيانات المعلوماتية المخزنة بها.

ب– أي جهاز تخزين معلومات يسمح بتخزين البيانات المعلوماتية في داخل النطاق المحلي.

2. إذا توافرت الأسباب الكافية للاعتقاد بأن المعلومات المطلوب البحث عنها وجدت مخزنة في شبكة معلومات أخرى أو في جزء آخر من تلك الشبكة الموجودة في إطار النطاق المحلي، فإنه يحق لتلك السلطات المختصة أن تمد التفتيش إليها بسرعة.

3. أن يمنح كل طرف السلطات المختصة صلاحية ضبط أو الحصول بطريقة مشابهة على البيانات المعلوماتية والتي تم الدخول على الشبكة من أجل الحصول عليها تطبيقاً للفقرة 1 ، 2.

وهذه الإجراءات تشمل الصلاحيات التالية :

. ضبط أو تأمين نظام الكمبيوتر.

. نقل وحفظ صورة من تلك البيانات المعلوماتية.

. المحافظة على كامل البيانات المعلوماتية المخزونة.

. العمل على منع أي أحد من الدخول أو أخذ هذه البيانات المعلوماتية من شبكة المعلومات المعنية.

أما عن التطبيق العملى الشرطى لمواجهة ظاهرة جرائم الإنترنت ، فقد قامت بريطانيا بتشكيل وحدة داخل جهاز الشرطة تسمى وحدة جرائم التكنولوجيا لمواجهة الخطر المتزايد للكمبيوتر وجرائم الإنترنت وتتخذ هذه الوحدة من لندن مقراً لها، وتضم بين أفرادها خبراء من الجامعات وبعض صناع الأجهزة الإليكترونية وعدد من أفراد أجهزة الأمن والمخابرات البريطانية ، فضلا عن ضباط الشرطة المتخصصين ويكون هدف هذه الوحدة هو التعامل مع أنواع مختلفة من الجرائم الحاسوبية التي تشمل الإحتيال والمواد الإباحية ، ونشاط الإستغلال الجنسي للأطفال ، ونشر الكراهية بسبب العرق أو التزوير ، والقمار ، والقرصنة وسرقة المعلومات ، وقرصنة البرمجيات وغسل الأموال ، والإتلاف بواسطة فيروسات الكمبيوتر (1).

أما الولايات المتحدة الأمريكية فقد قامت بإنشاء قسم خاص ضمن مكتب المباحث الاتحادي الأمريكي FBI أسمته IC3 (Internet Crime Complaint Center) مركز بلاغات جرائم الإنترنت. ويضم هذا المركز وكلاء مباحث ومحللين، وعلماء حاسوب، وأخصائيين في تكنولوجيا المعلومات، ويختص هذا المركز بتلقى الشكاوى الخاصة بعمليات الإختراقات التى تحدث عبر شبكة الإنترنت، والتى تصل إلى 20000 شكوى شهرياً، ومن ثم يقوم بتحليلها ومحاولة ضبط المخالفين وتقديمهم إلى القضاء، والعمل على إيجاد حلول ناجعة مستقبلا للحد من أي إختراقات جديدة قد تحدث(2).

وقد نشأ مركز الشكاوى الخاصة بجرائم الإنترنت كمفهوم سنة 1998 بإدراك ملائم بأن الجريمة بدأت تدخل الإنترنت لأن الأعمال التجارية والمالية كانت قد بدأت تتم عبر الإنترنت، ولأن مكتب التحقيقات الفدرالي أراد أن يكون قادراً على تعقب هذه النشاطات وعلى تطوير تقنيات تحقيق خاصة بجرائم الإنترنت ، ولم يكن هناك آنذاك أي مكان واحد معين يمكن للناس التبليغ فيه عن جرائم الإنترنت، وأراد مكتب التحقيقات الفدرالي التمييز بين جرائم الإنترنت والنشاطات الإجرامية الأخرى التي تُبلّغ عنها عادةً الشرطة المحلية ومكتب التحقيقات الفدرالي والوكالات

---

(1) Jason Bennetto , an article entitled Police launch a cyber squad to combat growth of Internet crime-available at: http://www.independent.co.uk/news/business/analysis-and-features/police-launch-a-cyber-squad-to-combat-growth-of-internet-crime-743235.html

(2) موقع مكتب التحقيقات الفيدرالى على الإنترنت www.fbi.gov

الأخرى التي تطبق القوانين الفدرالية[1].

ويعمل مركز الشكاوى عن كثب أيضاً مع المنظمة الكندية المسماة "الإبلاغ عن الجرائم الإقتصادية على خط الإنترنت" (RECOL) ويدير هذه المنظمة المركز القومي للجرائم المكتبية في كندا، وتدعمها شرطة الخيالة الملكية الكندية، ويعمل مركز الشكاوى الخاصة بجرائم الإنترنت كذلك مع المسؤولين عن تطبيق القانون في بلدان عديدة، بينها أستراليا والمملكة المتحدة. كما يحضر ممثلو مركز الشكاوى أيضاً اجتماعات دورية للمجموعة الفرعية حول جرائم التكنولوجيا المتقدمة التابعة لمجموعة الثماني (كندا، فرنسا، ألمانيا، إيطاليا، اليابان، روسيا والمملكة المتحدة والولايات المتحدة). ويعمل قسم من هذه المجموعة الفرعية على محاربة جرائم الإنترنت وتعزيز التحقيقات بشأنها [2].

ويهدف مكتب التحقيقات الفيدرالية فى مواجهته لجرائم الإنترنت إلى[3] :

. وقف التدخلات الأكثر خطورة على الشبكة والتى تتمثل فى إنتشار الشيفرات والفيروسات الخبيثة.

. تحديد وإحباط محاولات الأشخاص الذين يستخدمون الإنترنت لتلبية وإستغلال الأطفال جنسياً وإنتاج المواد الإباحية.

. مواجهة العمليات التي تستهدف الإعتداء على الملكية الفكرية.

. القضاء على الجريمة المنظمة عبر الوطنية وجرائم الإحتيال عبرالإنترنت.

ومن أبرز القضايا التى تعامل معها مكتب التحقيقات الفيدرالى ، ما تعرف بقضية الجحيم العالمي (GLOBAL HELL) ، حيث أطلق مجموعة من المخترقين على نفسهم هذا المسمى وتمكنت هذه المجموعة من إختراق مواقع البيت الأبيض والشركة الفيدرالية الأمريكية والجيش الأمريكي ووزارة الداخلية الأمريكية ، وقد أدين إثنين من هذه المجموعة جراء تحقيقات الجهات الداخلية في الولايات المتحدة ، وقد أمضى المحققون مئات الساعات في ملاحقة ومتابعة هذه المجموعة عبر الشبكة وتتبع آثار أنشطتها ، وقد كلف التحقيق مبالغ طائلة لما تطلبه من وسائل معقدة في المتابعة[4].

---

(1) Daniel Larkin, an article entitled fight cybercrime - available at : http://www. america.gov/st/democracy-arabic/2008/May/20081117124454snmassabla0. 260 1086. html
(2) Daniel Larkin , Ibid
(3) www.fbi.gov

(4) http://www.arab-elaw.com/show_similar.aspx?id=93

وكذلك وجه مكتب التحقيقات الفيدرالى الإتهام إلى ثلاثة أشخاص لحصولهم على بيانات بطاقات إئتمانية من خلال أجهزة الحاسب الآلى ، وإستغلالها فى سرقة ما يقارب على ثلاثة ملايين دولار من حسابات مصرفية لأكثر من ثلاثين ألف شخص ، وتعد هذه الواقعه على حسب ما جاء على لسان ممثل الإدعاء العام فى ولاية نيويورك أكبر قضية سرقة بالحاسب الآلى فى تاريخ الولايات المتحدة الأمريكية(1).

وفى واقعة أخرى قامت المباحث الفيدرالية بالقبض على 1500 شخص يشتبه فيهم بالتعامل فى دعارة الأطفال عبر شبكة الإنترنت وبث صور إباحية للقصر وذلك بعد ما قادت عمليات البحث والتقصى حول دعارة الأطفال عبر الإنترنت فى ألمانيا والمملكة المتحدة والولايات المتحدة إلى الكشف عن 200 ألف صورة إباحية لأطفال قصر (2).

وفي فرنسا يقوم فريق مكون من 13 شرطي بالإشراف على تنفيذ المهمات التي يعهد بها إليه وكلاء النيابة والمحققين وجمعيهم تلقوا تدريب متخصص إلى جانب إختصاصهم الأساسي في مجال التكنولوجيا الحديثة، وهم يقومون بموافقة المحققين أثناء التفتيش حيث يقومون بفحص كل جهاز وينقلون نسخة من الإسطوانة الصلبة وبيانات البريد الإلكتروني ثم يقومون بعمل تقرير يرسل إلى القاضي الذي يتولى التحقيق، أما عن المعدات والبرامج فهم يستخدمون برامج تستطيع إستعادة المعلومات من على الإسطوانة الصلبة كما يمكنها قراءة الإسطوانات المرنة والصلبة التالفة، كما يوجد تحت تصرفهم برامج تمكنهم من قراءة الحاسبات المحمولة(3).

أما فى مصر فقد تم إنشاء إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بالإدارة العامة للمعلومات والتوثيق وذلك بموجب القرار رقم 13507 لسنة 2002 ، والتى تهدف إلى ضبط مختلف صور الخروج علي الشرعية فيما يمس الأمن القومي وأمن الأفراد باستخدام الحواسب الآلية في مصر.

وتتكون الإدارة من ثلاثة أقسام على النحو التالى(4):

1. **قسم العمليات** : ويختص بالآتى:

. مكافحة الجرائم التى تقع بإستخدام أجهزة الحاسب الآلي في مجالات نظم وشبكات وقواعد

---

(1) www.gulfpark.com/showarticale.php?cat=news&article-id=252

(2) أنظر فى ذلك د. عمر محمد أبو بكر بن يونس ، الجرائم الناشئة عن إستخدام الإنترنت ، رسالة دكتوراه ، كلية الحقوق ، جامعة عين شمس ، 2004 ، ص456.

(3) د. صالح أحمد البربري ، المرجع السابق ، ص8.

(4) موقع وزارة الداخلية المصرية على الإنترنت http://citizen-service.moiegypt.gov.eg/crimes_web/main.htm

البيانات.

. إخطار الأجهزة النوعية المختصة بأعمال المكافحة بالبيانات والمعلومات المتعلقة بالجرائم الجنائية التى يمكن التوصل إليها من خلال الإتصال بشبكات المعلومات والتنسيق معها.

. إعداد قاعدة بيانات بجرائم المعلومات التى تدخل في نطاق إختصاص الإدارة والأحكام الصادرة فيها.

2. **قسم التأمين** : ويختص بالآتى:

. وضع الخطط والأساليب التى تستخدم في مجال تأمين نظم المعلومات والشبكات الخاصة بأجهزة الوزارة.

. تقديم العون لكافة أجهزة الوزارة التى تطلب تأمين نظم معلوماتها وشبكاتها حماية للثروة المعلوماتية بها .

. متابعة التراخيص التي تصدر للشركات الخاصة في مجال نظم وأجهزة وشبكات المعلومات وذلك بالتنسيق مع الجهات المعنية .

3. **قسم البحوث والمساعدات الفنية** : ويختص بالآتى:

. القيام بإعداد البحوث الفنية والقانونية في مجال تأمين نظم وشبكات المعلومات بالحاسبات الآلية.

. بحث مدى ملاءمة التشريعات الجنائية لمواجهة جرائم المعلومات التى تدخل في مجال عمل الإدارة وإقتراح التوصيات.

. تقديم الدعم الفني لجميع جهات الوزارة في كافة القضايا والوقائع المرتبطة بمجال نظم وبرامج وأجهزة و شبكات المعلومات.

. توفير كافة المساعدات الفنية وإبداء الرأى والمشورة للجهات سواء من داخل الوزارة أو خارجها للمعاونة في عمليات ضبط الجرائم التى تتم بإستخدام الحاسب الآلي.

وقد تمكنت الإدارة المذكورة من إحباط عدد من المحاولات الإجرامية التى تتم بإستخدام شبكة الإنترنت ، تمثل أغلبها فى إختراق مواقع للإنترنت ، سرقة أرقام بطاقات الإئتمان ، قذف وسب وإساءة سمعة ، تهديد وإبتزاز ، نصب وإحتيال ، محاولة كسر شفرات القنوات الفضائية عن طريق الإنترنت ، الإعتداء على حقوق الملكية الفكرية ، أعمال منافية للآداب.

إضافةً لذلك فإن الإدارة العامة لمباحث الأموال العامة تلعب دوراً بارزاً كذلك فى مجال مكافحة جرائم الإنترنت المالية ، ولقد قامت الإدارة المذكورة بإحباط العديد من المحاولات الإجرامية ونذكر منها على سبيل المثال القبض على شخصين يحملان الجنسية النيجيرية قاما بإرسال رسالة إليكترونية لأحد المواطنين ، مفادها أنه فاز مع أحد شركات اليانصيب على الإنترنت والموجودة فى هولندا بجائزة مالية قدرها "750 ألف دولار أمريكى" ومطالبتة بدفع مبالغ مالية كرسوم إدارية لإنهاء إجراءات إستلامه الجائزة وبالفعل قام بتحويل مبلغ (3721) دولار أمريكى على العنوان المرسل إليه بالرسائل الواردة إليه على بريده الإليكترونى ، وبعد ذلك تلقى رسالة أخرى تفيد حضور شخصين للقاهرة لتسليمة الجائزة ، وعند مقابلتة طلب منه مبلغ 2800 دولار قيمة تحويل مبلغ الجائزة إليه بالقاهرة، تشكك المواطن فى الأمر وبإبلاغ الإدارة تم ضبط الشخصين.

إضافةً لذلك فقد نظمت وزارة الداخلية فى مصر ندوة بعنوان "المواجهة الأمنية للجريمة المعلوماتية" والتى ركزت على أهمية الدور الشرطى فى مواجهة جرائم المعلوماتية وقد جاء فى توصيات الندوة ضرورة[1]:

. إدراج موضوعات الجريمة المعلوماتية وسبل مكافحتها ضمن المناهج الدراسية بكليات ومعاهد الشرطة، بما يحقق تدعيم الجهود الأمنية المبذولة في هذا الشأن.

. تحديث وتطوير البرامج التدريبية الهادفة إلى تنمية قدرات العاملين في مجال مكافحة الجريمة المعلوماتية، والإستمرار في إيفاد الكوادر المتخصصة للخارج للاطلاع على التجارب الناجحة في هذا المجال.

. تدعيم دور أجهزة إنفاذ القانون فى مواجهة الجريمة المعلوماتية من خلال الإستمرار فى تعزيز الإمكانيات المادية والبشرية المتاحة لها.

. تبادل الخبرات والمعلومات وتكثيف المشاركة في المؤتمرات الدولية والندوات والحلقات العلمية ذات الصلة ومتابعة المستجدات الدولية في مجال مكافحة الجرائم المعلوماتية.

. الدعوة إلى وضع آلية تشريعية تحدد ماهية الجريمة المعلوماتية وأركانها والعقوبات المقررة لها بما يكفل تحقيق التوازن بين حق المجتمع فى التداول الحر للمعلومات وحماية الكيان الإجتماعي.

---

(1) راجع فيما يخص هذه الندوة موقع وزارة الداخلية المصرية على الإنترنت
http://www.moiegypt.gov.eg/Arabic/Departments+Sites/Media+and+public+Relation/Conferences/mo07042009.htm

. إعادة النظر بتشديد العقوبات في القوانين ذات الصلة بالجريمة المعلوماتية بما يكفل الإستخدام الآمن والمشروع لتكنولوجيا المعلومات.

. إرتياد آفاق جديدة في مجال التعاون الدولى لمكافحة الجريمة المعلوماتية من خلال الإنضمام أو إبرام الإتفاقيات الدولية ذات الصلة.

وفى سلطنة عمان أولت الشرطة هناك إهتماماً بالغ الأهمية لجرائم الحاسب الآلى والإنترنت وذلك من خلال[1]:

. إنشاء قسم خاص بالجرائم الإليكترونية يتبع لإدارة الجرائم الإقتصادية بالإدارة العامة للتحريات والتحقيقات الجنائية وذلك فى العام 2004.

. عقد العديد من الندوات والدورات أو المشاركة فيها وذلك بالتعاون مع بعض الجهات المختصة من أجل نشر الوعى والتنبيه بمخاطر هذه الجرائم.

. إعداد الدراسات والبحوث والإحصائيات السنوية حول الجرائم الإليكترونية التى تمت أو تتم فى السلطنة.

. التنسيق والتعاون مع السلطات المختصة سواء فى الدول الأخرى أو مع الهيئات والمنظمات الدولية والإقليمية من أجل تبادل الخبرات فى مجال مكافحة هذا النوع المستحدث من الجرائم كلجنة أمناء العرب والإنتربول.

([1]) د.حسين بن سعيد الغافرى ، بحث بعنوان جهود السلطنة فى مواجهة جرائم الإنترنت ، ص12 ، البحث منشور بالموقع : http://www.eastlaws.com/Others/ViewMorafaat.aspx?ID=24

المبحـــث الثانـــى

مكافحة جرائم الإنترنت على المستوى الدولى

ذكرنا سلفاً أن جرائم الإنترنت يصعب مواجهتها على الصعيد الداخلى أو الوطنى فقط نظراً لتشعب خيوطها وإمكانية إرتكابها داخل أكثر من دولة فى نفس الوقت ، الأمر الذى أوجب ضرورة التعاون الدولى بشتى أنواعه للقضاء أو على أقل تقدير الحد من هذه الجرائم وتحجيمها.

وقد أكدت إتفاقية بودابست على أهمية التعاون الدولى فى مجال مكافحة جرائم الكمبيوتر حيث نصت المادة 23 من على أن يتعاون الأطراف مع بعضهم البعض، وفقاً لنصوص هذا الباب على تطبيق الوسائل الدولية الملائمة بالنسبة للتعاون الدولي في المجال الجنائي والترتيبات التي تستند إلى تشريعات موحدة ومتبادلة وكذلك بالنسبة للقانون المحلي على أوسع نطاق ممكن بين بعضهم البعض بغرض التحقيقات والإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية وكذلك بشأن الحصول على الأدلة في الشكل الإلكتروني لمثل هذه الجرائم.

وعليه سنتناول دراسة هذا المبحث من خلال ثلاث مطالب وهى على التوالى:

المطلب الأول : التعاون الشرطى والقضائى على المستوى الدولى.

المطلب الثانى : الإتفاقيات والمؤتمرات الدولية.

المطلب الثالث : معوقات التعاون الدولى.

المطلـــب الأول

التعاون الشرطى والقضائـى على المستوى الدولى

الفـــرع الأول

التعاون الشرطـى على المستوى الدولى.

يحدث التعاون الشرطى على المستوى الدولى عند إتفاق الإدارات الشرطية المعنية بجرائم المعلومات والإنترنت فى أكثر من دولة على إتباع سياسة عامة وموحده فى مجال التحقيقات وجمع الأدلة وتبادل المعلومات وذلك إذا ما تعدت آثار جرائم الإنترنت الحدود الإقليمية لأكثر من دولة.

والسبب فى ذلك أنه من الصعب على الدولة بمفردها القضاء على جرائم المعلوماتية عابرة الحدود ، لأن جهاز الشرطة فى هذه الدولة أو تلك يصعب عليه تعقب المجرمين ومتابعتهم إذا ما عبروا حدود الدولة ، ولذلك فإن الحاجة ملحة إلى تعاون أجهزة الشرطة بين الدول وتنسيق العمل فيما بينها لضبط المجرمين ومكافحة نشاط الإجرام المعلوماتى الذى يتجاوز حدود الدولة[1].

وجدير بالذكر أن البدايات الأولى للتعاون الشرطى الدولى . بشكل عام . ترجع إلى العام 1904 عندما تم إبرام الإتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض ، وكذلك أخذ التعاون الشرطى الدولى صورة المؤتمرات الدولية وتمثل ذلك فى مؤتمر موناكو فى عام 1904 كذلك ، والذى ضم بدوره رجال شرطة وقضاء من 14 دولة ، لمناقشة ووضع أسس التعاون الدولى فى بعض المسائل الشرطية ، وبعد إنتهاء الحرب العالمية الأولى وتحديداً فى العام 1919 حاول الكولونيل فان هوتين أحد ضباط الشرطة الهولندية إحياء فكرة التعاون الدولى وذلك بالدعوة لعقد مؤتمر دولى لمناقشة هذا الموضوع غير أنه لم يوفق فى مسعاه[2].

وتبلور بعد ذلك التعاون الشرطى الدولى وقد أخذ عدة صور كالآتى:

1 ـ المنظمة الدولية للشرطة الجنائية (الإنتربول):

الإنتربول هو منظمة عالمية أنشئت في عام 1923 وتتكون هذه المنظمة من قوات الشرطة لأكثر من 188 دولة وهو بذلك يعد أكبر منظمة شرطية في العالم ، وتتخذ المنظمة من

([1]) د. طارق إبراهيم الدسوقى عطية ، الأمن المعلوماتى (النظام القانونى لحماية المعلوماتى) ، المرجع السابق ، 593 . 594.

(2) راجع فى ذلك ، د.حسين بن سعيد الغافرى ، السياسة الجنائية فى مواجهة جرائم الإنترنت (دراسة مقارنة) ، رسالة دكتوراه ، كلية الحقوق ، جامعة عين شمس ، ص503 . 504.

مدينة ليون بفرنسا مقراً رئيسياً لها ، ومن الجدير بالذكر أنه فى بداية عمل هذه المنظمة كان المركز الرئيسى لها هو فيينا. وقد توقفت المنظمة عن العمل بسبب إندلاع الحرب العالمية الثانية وبعد ذلك أعيد تنْظيِم المنظمة من جديد عام 1946م وإنتقلت إلى باريس، قبل أن تنتقل للمرة الأخيرة بعد ذلك فى مقرها بمدينة ليون.

وللإنتربول خدمات ووظائف عدة تتلخص فى[1]:

أ . **خدمات إتصال شرطي عالمي مأمون** : يتدبر الإنتربول منظومة إتصالات شرطية عالمية تتيح لموظفي إنفاذ القانون المرخص لهم في جميع البلدان الأعضاء طلب معلومات شرطية هامة وإحالتها والوصول إليها بشكل آني ومأمون.

ب . **خدمات بيانات ميدانية وقواعد بيانات للشرطة** : يتدبّر الإنتربول مجموعة من قواعد البيانات التي تحتوي على معلومات أساسية كأسماء الإرهابيين المشتبه بهم، وصور الإعتداء الجنسي على الأطفال، وبصمات الأصابع ، ووثائق السفر المسروقة والمفقودة، والأشخاص المطلوبين.

جـ . **خدمات الإسناد الشرطي الميداني** : حدّد الإنتربول عدة مجالات إجرام ذات أولوية وهو يركز موارده عليها وهي الفساد، والمخدرات والإجرام المنظم، والإجرام المالي والمرتبط بالتكنولوجيا المتقدمة، والمجرمون الفارون، والأمن العام والإرهاب، والإتجار في البشر.

د . **التدريب والإنماء الشرطي** : يقدم الإنتربول لأجهزة الشرطة الوطنية برامج تدريبية محددة لتعزيز قدرة البلدان الأعضاء على مكافحة الإجرام الخطر العابر للحدود والإرهاب بشكل فعّال.

وجدير بالذكر أن قانون الإنتربول الأساسي يحظر على المنظمة أي تدخّل أو نشاط ذي طابع سياسي أو عسكري أو ديني أو عنصري ، والقصد من ذلك هو تيسير التعاون الشرطي الدولي حتى في غياب العلاقات الدبلوماسية بين بلدان معينة ، وتتخذ جميع الإجراءات ضمن حدود القوانين السارية في مختلف البلدان وبروح الإعلان العالمي لحقوق الإنسان.

وقد أدرك الإنتربول خطورة الجرائم السيبرانية منذ منتصف العقد الأخير من القرن الماضى وإستضاف فى عام 1995 المؤتمر الدولى الأول بشأن الجرائم الحاسوبية ، وأنشأ المؤتمر داخل الإنتربول وحدة مركزية وأربعة فرق عاملة معنية بالجرائم المتصلة بالتكنولوجيا الراقية مثلت أفريقيا ، الأمريكتين ، آسيا ، وأوروبا ، وتختص هذه الفرق بإتاحة التدريب والتعاون على المستوى الإقليمى لدول كل قارة ، ومن أجل ذلك أصدر الإنتربول كتيباً إرشادياً للمحققين

---

(1) أنظر موقع الإنتربول على الإنترنت : http://www.interpol.int.

الجدد فى الجرائم السيبرانية ودليلاً أكثر تفصيلاً يعرض للصعوبات التى يمكن أن تواجه أجهزة إنفاذ القوانين ويبين أفضل الممارسات والتقنيات التى يجب على المحققين القيام بها لتخطى هذه الصعوبات[1].

وقد أكدت شرطة الإنتربول على ضرورة التعاون الدولى فى مكافحة جرائم الإنترنت وذلك فى مؤتمر جرائم الإنترنت المنعقد فى لندن بالعام 2000 ، من خلال الكلمة التى ألقاها سكرتير الإنتربول (ريموند كيندل) والتى أكد فيها على أنه يجب على المجتمع الدولى عدم الإنتظار إلى حين عقد معاهدات وإتفاقيات فى هذا الإطار بل يجب الشروع وبشكل فورى فى مكافحة هذه الجرائم[2].

وقد أطلق الإنتربول في عام 2008 المبادرة الأمنية العالمية للقرن الحادي والعشرين التي تلخص منظور المنظمة الإستراتيجي فى بعض المسائل والتى يأتى على رأسها الإجرام السيبري أو إجرام الإنترنت ، والعمل على مكافحتها من منظورعالمي فالمبادرة الأمنية العالمية تهدف إلى التصدي لهذه التحديات الأمنية الدولية.

إضافةً لذلك فقد أنشأ الإنتربول بنك الإنتربول للصور المتعلقة بإنتاج المواد الإباحية، ويكون في متناول كل قوات الشرطة، على أن يحتوي على صور الأطفال الذين تم التعرف عليهم على مواقع إباحية للأطفال عبرالإنترنت وتقدم قاعدة البيانات هذه معلومات إلى الشخص المخول من قِبل البلد التي ينتمي إليها هذا الطفل وعناوين عناصر الشرطة المتخصصة، مع مراعاة عنصر سرية هوية هذا الطفل ومن جهة أخرى، يتم الإشارة إلى سن الطفل، وهي معلومة ثمينة تُمكِّن من إيجاد عنصر من أهم عناصر الجريمة وبهذه الطريقة يتم التوفيق بين كل من فعالية المتابعة القضائية وإحترام كرامة الطفل[3].

ولقد تعاونت شرطة الإنتربول مع الشرطة الفرنسية ومكتب التحقيقات الفيدرالى FBI فى إحدى قضايا مكافحة إستغلال الأطفال في إنتاج المواد الإباحية على الإنترنت وهى العملية المسماة بعملية فالكون (FALCON) في إبريل 2005 ، والتي سمحت بتفكيك شبكة إجرامية

---

(1) اللواء د. محمد فتحى عيد ، الإنترنت ودوره فى إنتشار المخدرات ، أكاديمية نايف العربية للعلوم الأمنية ، الرياض ، 1424هـ ، ص185.

(2) د.عمر محمد أبوبكر بن يونس ، المرجع السابق ، ص 814.

(3) جان فرانسوا هنروت ، أهمية التعاون الدولى والتجربة البلجيكية فى تبادل المعلومات بين عناصر الشرطة والتعاون القضائى ، بحث مقدم إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر ضمن برنامج تعزيز حكم القانون فى بعض الدول العربية " مشروع تحديث النيابات العامة" ، المملكة المغربية ، فى الفترة من 20.19 يونيو 2007، ص110.

تنشط في العديد من الدول الأوروبية[1].

2 ـ الشرطة الأوروبية المشتركة (اليوروبول):

اليوروبول هى وكالة متخصصة لإنفاذ القانون الأوروبي ، تم الإتفاق على إنشائها فى إتفاقية الإتحاد الأوروبى المسماة بإتفاقية ماسترخت المبرمة فى عام 1991 قبل أن تدخل حيز التنفيذ فى 1992/2/7، ومقر مكتب هذه الوكالة هو لاهاى بهولندا ويعمل فيه موظفو جمارك وقوات من الشرطة. وتتحصرمهمة الوكالة الأساسية فى مساعدة الدول الأعضاء في الإتحاد الأوروبي فى التصدى لمجموعة كبيرة من الجرائم الدولية والتى يأتى من ضمنها الإستغلال الجنسي للنساء والأطفال والأفلام والمواد الإباحية وتبييض الأموال وتزوير اليورو[2].

وقد أعطى الإتحاد الأوروبى لجهاز اليوروبول حق مشاركة السلطات الوطنية فى سياستها المقررة لمكافحة الجريمة المنظمة وإعداد الإجراءات فى مجال التحقيقات الشرطية ، الجمركية ، القضائية ، للعمل مع سلطات تلك الدول كوحدة متكاملة ، ومن بين صلاحياته أن يطلب من الدول الأعضاء التدخل فى التحقيقات التى باشرتها وحضور جلسات التحقيق المتعلقة بالجريمة المنظمة، كما يقوم الجهاز بتحليل المعلومات المتعلقة بالجريمة المنظمة فى صورها المختلفة[3].

ولقد قادت اليوروبول عدة عمليات فى مجال جرائم الإنترنت ، من أبرزها عملية أوديسيوس (Odysseus) التي تمت في 26 فبراير 2004 بمبادرة من يوروبول، وقامت قوات الشرطة خلالها بعمليات شملت 10 دول هي(أوستراليا، بلجيكا، كندا، ألمانيا، هولندا، النرويج، بيرو، أسبانيا، السويد ، بريطانيا) [4].

وكذلك عملية محطم الجليد (Icebreaker) في 14 يونيو 2005 ، والتى تم خلالها مداهمة وتفتيش أماكن في ثلاث عشرة دولة أوروبية هي(النمسا، بلجيكا، فرنسا، ألمانيا، المجر، أيسلندا، إيطاليا، هولندا، بولونيا، البرتغال، سلوفاكيا، السويد، وبريطانيا العظمى) كما تم توقيف أفراد في كل من فرنسا، بلجيكا، المجر، وأيسلندا والسويد[5].

---

(1) جان فرانسوا هنروت ، المرجع السابق، ص108.

(2) موقع الشرطة الأوروبية على الإنترنت : http://www.europol.europa.eu

(3) د. فائزة يونس الباشا ، الجريمة المنظمة في ظل الإتفاقيات الدولية والقوانين الوطنية ، دار النهضة العربية ، الطبعة الأولى ، 2001 ، ص354.

(4) جان فرانسوا هنروت ، المرجع السابق،108.

(5) جان فرانسوا هنروت ، المرجع السابق، 108.

3- نظام شنغن:

نظام معلومات شنغن، هو قاعدة بيانات مقرها مدينة ستراسبورج تمكّن قوات الشرطة والسلطات القضائية من تبادل المعلومات حول الأشخاص الذين تصدر بحقهم مذكرات توقيف أو طلبات تسليم المطلوبين.

ولقد تم إستحداث هذا النظام بناءً على إتفاقية شنغن الموقعة في 14 /6/ 1985، من خلال خمس دول أوروبية (بلجيكا ، فرنسا ، ألمانيا الغربية ، لوكسمبورغ ، وهولندا)، ويضمن هذا النظام تعزيز التعاون الشرطي الأوروبي فى مجالى مراقبة المشتبه فيهم عبر الحدود وملاحقة المجرمين دولياً ويعرف هذا النظام بإسم SIS (systeme d information schengen)[1].

ويظهر ذلك جلياً فى المادتين 40 و41 من الإتفاقية المذكورة ، حيث أن المادة 40 تعطى الحق لرجل الشرطة الذى تكون دولته طرفاً فى الإتفاقية الحق فى مراقبة أى شخص يشتبه قى إرتكابه جريمة ما متواجد فى إقليم دولة أخرى طرف فى الإتفاق ، وذلك بشرط الحصول على إذن مسبق من الدولة التى سيتم فيها الإجراء وأن تكون من الجرائم التى يجوز فيها تسليم المجرمين بإستثناء حالة الضرورة والتى يجوز فيها لرجل الشرطة ممارسة مهامه دون الحصول على هذا الإذن ، والإجراءات التى يجوز لرجل الشرطة القيام بها خلال عملية المراقبة هى المعاينة وإقتفاء أثر المشتبه به وسماع الشهود إختيارياً[2].

أما المادة 41 فهى تعطى الحق فى ملاحقة المجرمين خارج الحدود وذلك فى حالتين فقط ، الأولى هى حالة التلبس أما الحالة الثانية فهى حالة هرب شخص محبوس ، وذلك أيضاً مشروط بأن تكون الدولة التى سيتم فيها الإجراء طرفاً فى الإتفاقية[3].

ومن الجدير بالذكر أنه على المستوى الأوروبى كذلك ، وفى 12 أبريل 1996 تم عقد إجتماع ضم وزراء الداخلية والعدل والمالية للدول أعضاء الإتحاد الأوروبى كان من ضمن أهدافه تحسين التعامل بين الأجهزة الشرطية وفى سبيل ذلك أسند إلى منظمة الإنتربول العمل

---

(1) http://www.delsyr.ec.europa.eu/ab/europe_in_12_lessons/10.html

(2) راجع فى ذلك ، نبيلة هبة هروال ، مرجع سابق ، ص 162 . 163.

(3) راجع فى نفس المعنى ، نبيلة هبة هروال ، مرجع سابق ، ص163.

على تحقيق الأهداف التي حددها هذا الإجتماع ، وهي:[1]

. ضمان المساعدة المشتركة لسلطات الشرطة الجنائية وتنميتها وتطويرها في نطاق أوسع وفي إطار قوانين الدول المختلفة لصالح حماية حقوق الإنسان .

. تأسيس مراكز قادرة على الإسهام بفاعلية في الوقاية وردع إنتهاكات القوانين المشتركة وتطوير تلك المراكز والعمل على على رفع مستوى أجهزتها لتنفيذ القوانين في مختلف المجالات ، من تبادل المعلومات إلى التحري والملاحقة القضائية والإفادة من التقنية والتنظيم.

4 - الأورجست:

وهو جهاز يوجد على المستوى الأوروبي يساعد على التعاون القضائي والشرطي في مواجهة ومكافحة جميع أنواع الجرائم الخطيرة والتى من ضمنها جرائم الإنترنت تم إنشاؤه في عام 2002 ، وتتلخص نشاطاته فى تحسين التنسيق والتعاون بين السلطات القضائية المختصة للدول الأطراف ، وتبادل المعلومات فيما بين الدول الأعضاء فى الإتحاد الأوروبى[2].

الفـرع الثانـى
التعـاون القضائـى على المستوى الـتدولى

التحقيق فى جرائم الإنترنت يختلف عن التحقيق فى غيرها من الجرائم نظراً لما يفردها ويميزها من خصائص والتى من ضمنها أنها جريمة قد تجوب الحدود الإقليمية لأكثر من دولة ، وبالتالى تولدت الحاجة لأن تكون هناك مساعدة رسمية من السلطات في البلد الذي كان منشأ الجريمة، أو من السلطات في البلدان التي عَبَر من خلالها النشاط المجرَّم وهو في طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة.

وتبرز أهمية التنسيق القضائى بين الدول وذلك لعدة أسباب[3]:

. على المستوى الدولي لم يبدأ بعد النظربشكل متعمق في مسائل الإجراءات العقابية المتعلقة بتكنولوجيا الإعلام والاتصال إلا في التسعينيات، ولهذا فإنه ليس من الغريب أن عددا كبيرا من الدول ليس لديها نظام دولي يُعنى بوضع القوانين في هذا المجال.

---

(1) د.أبو المعالي محمد عيسى ، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية ، بحث مقدم إلى المؤتمر المغاربي الأول حول (المعلوماتية والقانون) ، المنعقد في الفترة من 29.28 أكتوبر 2009 ، أكاديمية الدراسات العليا ، طرابلس ، ليبيا ، ص14.

(2) راجع فى ذلك ، نبيلة هبة هروال ، المرجع السابق ، ص 159 . 160.

(3) جان فرانسوا هنروت ، المرجع السابق ، ص97.

. يعتبر تنسيق الأنظمة الفعّالة أمرا أساسيا وعاجلا لتجنب نشوء ما يطلق عليه الملاذ الرقمي(بمعنى إتخاذ الإنترنت ملاذاً لممارسة الجريمة)وقد تم إطلاق سراح أونيل دو غوزمان ، الذي وضع فيروس "I love you" وأُسقطت التهم الموجهة إليه من طرف الحكومة الفلبينية وذلك لأن قانون الفلبين في تلك الفترة لم يكن يُجرم هذه الأفعال.

. يشكل هذا التنسيق في حد ذاته القاعدة اللازمة لإقامة تعاون دولي فعال ومن شأن وجود مثل هذه القوانين الإجرائية الفعالة أن يجعل عملية التعاون تسير بشكل آلي وسهل، حتى أنه من المفضل بالطبع إتخاذ إجراءات أخرى لتسهيل عملية بناء هذا التعاون وتعتبر عملية تجريم الفعل من كلا الطرفين الأساس القانوني الذي يتحدد بناء عليه قبول أو رفض التعاون بين الطرفين، فقد يحدث الخلاف عندما يكون قانون العقوبات للدولة متلقية الطلب بتسليم الجُناة لا يعاقب على مثل هذه الأفعال المرتكبة والتي دفعت بالدولة مقدمة الطل إلى التقدم بطلب التسليم لذا، من الضروري تنسيق عملية التجريم إذا ما كنا نريد تفادي حدوث هذا الخلاف.

وبناءً على ما سبق فإن المساعدة الرسمية المتبادلة هي عملية أكثر تعقيداً يتم اللجوء إليها عادة عملاً بإتفاقيات بين البلدان المعنية ونصوص قانونية داخلية. وهي تشترط في الغالب الأعم أن تكون الجريمة على درجة معينة من الخطورة ، وأن تشكل جريمة في كل من البلدان الطالبة والموجه إليها الطلب ، ويشار إلى هذا الأمر الأخير باعتباره تجريماً مزدوجاً[1].

وتعرف المساعدة المتبادلة والمعروفة فى هذا الصدد بالمساعدة القضائية الدولية بأنها إجراء قضائى تقوم به دولة ما ، من شأنه تسهيل مهمة المحاكم فى دولة أخرى ، بصدد جريمة من الجرائم[2].

ويشكل عام فإن المساعدة القضائية الدولية تتحقق بالخطوات التالية[3]:

1 . **الطلب :** وتقدمه الدولة صاحبة الإختصاص الجنائى بالمحكمة ، ويخضع هذا الطلب لقانون الدولة الطالبة وفى نطاق الإتفاقية التى تعقدها مع الدولة التى ستقدم المساعدة ، ويتم تقديم الطلب بالطرق الدبلوماسية بحسب الاصل ، ومع ذلك فإن بعض الإتفاقيات الدولية تسمح باللإتصال المباشر بين جهات العدل فى الدولتين كسباً للوقت.

---

(1) د.موسى مسعود ارحومة ، السياسة الجنائية في مواجهة جرائم الإنترنت ، بحث مقدم إلى مؤتمر التنمية البشرية في عالمٍ متغير، جامعة الطفيلة (الأردن) فى الفترة من 10-2007/7/12، ص4.

(2) سالم محمد سليمان الأوجلى ، أحكام المسئولية الجنائية عن الجرائم الدولية فى التشريعات الوطنية ، دراسة مقارنة (رسالة دكتوراه) كلية الحقوق ، جامعة عين شمس ، 1997 ، ص425.

(3) د. حسنين إبراهيم صالح عبيد ، القضاء الجنائى الدولى ، (تاريخه . تطبيقاته . مشروعاته) ، دار النهضة العربية ، 1977 ، ص140، مشار له لدى ، سليمان أحمد فضل ، المرجع السابق ، ص421.

2 . **فحص الطلب** : وتقوم به الدولة التى ستقدم المساعدة ، ويتم ذلك عن طريق التحقق من إعتبار الواقعة المطلوب تحقيقها تعد جريمة وفقاً لقانون الدولة الطالبة ، وفى ضوء مدى إختصاص الدولة المطلوب منها بإجابة هذا الطلب وفقاً لنصوص الإتفاقية التى تعقدها مع الدولة الطالبة.

3 . **تنفيذ المساعدة القضائية** : ويتم وفقاً لقواعد الدولة المطلوب منها ، فالإجراء يتم وفقاً لقانون الدولة التى تنفذه.

وتتخذ المساعدة القضائية أكثر من صورة على النحو التالى:

- **الصورة الأولى: تبادل المعلومات:**

وهو يشمل تبادل المعلومات والوثائق التى تطلبها سلطة قضائية أو أمنية أجنبية بصدد جريمة ما ،عن الإتهامات التى وجهت إلى رعاياها فى الخارج والإجراءات التى أتخذت ضدهم كما أن هناك مظهر آخر لتبادل المعلومات يتعلق بالسوابق القضائية للجناة ، من خلالها تتعرف الجهات القضائية بدقة على الماضى الجنائى للفرد المحال إليها ، وهى تساعد فى تقرير الأحكام الخاصة بالعود ، ووقف تنفيذ العقوبة ، وعدم الأهلية ، إلا أن تدويل الصحيفة الجنائية مازال فى مراحله الأولى ، وتقوم الدول بإعدادها بالنسبة لرعايا الدول التى ترتبط بها بإتفاقيات تبادل معلومات[1].

ولقد أوصى مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين، بتطوير التبادل المنهجي للمعلومات بوصفه عنصراً رئيسياً من عناصر خطة العمل الدولية لمنع الجريمة ومكافحتها ، وأوصى بأنه على منظمة الأمم المتحدة أن تنشئ قاعدة معلوماتية للإعلام الدول الأطراف بالاتجاهات العالمية في مجال الجريمة[2].

وفى هذا الصدد يجب ألا تحول مركزية المعلومات دون نشرها وتبادلها فيما بين الدول ، بعد ترتيبها ودراستها ومعالجتها ، على النحو الذى يسمح بالإفادة منها في مرحلة التحقيقات والمحاكمة ، ولمتابعة الأشخاص المشبوهين سواء أكانوا أشخاصاً أم هيئات ، مع كفالة الحريات الشخصية ، وتشمل كذلك ما يتعلق بتحركات المجرمين المنظمين في جماعة إجرامية عبر الحدود وما يتعلق بالوثائق المزورة والمسروقة التي قد يلجأون إلى استخدامها وكافة المعلومات المتصلة بما يرتكبونه من أنشطة إجرامية ، للتنسيق فيما بين أجهزة مكافحة التهريب المنظم

(1) د. سليمان أحمد فضل ، مرجع سابق ، ص422.

(2) د.أبو المعالي محمد عيسى ، المرجع السابق ، ص7. 8.

للأشخاص عبر الحدود الوطنية(1).

وفى سبيل تبادل المعلومات نصت إتفاقية المنظمة الدولية العربية للدفاع الإجتماعى ضد الجريمة فى المادة 7 فى الفقرتين د ، هـ على:

(د) تبادل المعلومات والبيانات والإحصائيات والمطبوعات.

(هـ) الإتصال بالهيئات والمؤتمرات الدولية والتعاون معها في كل ما يخدم أغراض المنظمة.

ونصت كذلك إتفاقية الرياض العربية للتعاون القضائى على تبادل المعلومات بنصها فى المادة الأولى من الإتفاقية على: (تتبادل وزارات العدل لدى الأطراف المتعاقدة بصفة منتظمة نصوص التشريعات النافذة والمطبوعات والنشرات والبحوث القانونية والقضائية والمجلات التي تنشر فيها الأحكام القضائية ، كما تتبادل المعلومات المتعلقة بالتنظيم القضائي ، وتعمل على إتخاذ الإجراءات الرامية إلى التوفيق بين النصوص التشريعية والتنسيق بين الأنظمة القضائية لدى الاطراف المتعاقدة حسبما تقتضيه الظروف الخاصة بكل منها).

ونصت كذلك الإتفاقية المذكورة فى المادة 5 ، على تبادل صحف الحالة الجنائية بنصها : (ترسل وزارة العدل لدى طرف متعاقد إلى وزارة العدل لدى أي طرف متعاقد آخر بيانات عن الأحكام القضائية النهائية الصادرة ضد مواطنيه أو الأشخاص المولودين أو المقيمين في إقليمه والمقيدة في صحف الحالة الجنائية (السجل العدلي) طبقا للتشريع الداخلي لدى الطرف المتعاقد المرسل. وفي حالة توجيه إتهام من الهيئة القضائية أو غيرها من هيئات التحقيق والإدعاء لدى أي من الأطراف المتعاقدة ، يجوز لأي من تلك الهيئات أن تحصل مباشرة من الجهات المختصة على صحيفة الحالة الجنائية (السجل العدلي) الخاصة بالشخص الموجه إليه الإتهام. وفي غير حالة الإتهام يجوز للهيئات القضائية أو الإدارية لدى أي من الأطراف المتعاقدة الحصول من الجهات المختصة على صحيفة الحالة الجنائية (السجل العدلي) الموجودة لدى الطرف المتعاقد الآخر ، وذلك في الأحوال والحدود المنصوص عليها في تشريعه الداخلي).

وكذلك نصت إتفاقية التعاون القضائي بين الأردن وسوريا فى المادة 21 على تبادل المعلومات الجزائية بنصها:

1. تتبادل دائرتا السجل العدلي في الدولتين المعلومات عن الجنح والجنايات المحكوم بها في إحداها ضد رعايا الدولة الاخرى.

2. تعطي كل من الإدارتين مجانا الإدارة الثانية ما تطلبه من معلومات مستقاة من السجل

---

(1) د.أبو المعالي محمد عيسى ، المرجع السابق ، ص8.

العدلي.

ومن الخطوات السباقة لتبادل المعلومات حول جرائم الإنترنت قيام اليابان بتمويل إقامة شبكة للإتصال المستند إلى الإنترنت تضم 21 بلداً آسيوياً من أجل تبادل المعلومات حول الجرائم السيبرانية[1].

وقد نصت إتفاقية بودابست على المساعدة المتبادلة بين الدول الأطراف فى الإتفاقية وذلك لأغراض التحقيقات أو الأجراءات المتعلقة بالجرائم ذات العلاقة بنظم وبيانات الكمبيوتر ، أو جمع أدلة الجريمة فى شكل إليكترونى ، على أن يتم ذلك وفقاً لقانون الدولة المطلوب منها تقديم المساعدة أو إتفاقيات تبادل المساعدة المبرمة بين الأطراف إن وجدت.

وقد ذكرت المادة فى فقرتها الثالثة طرق تبادل المساعدات فى الحالات الطارئة والتى قد تتمثل فى أجهزة الفاكس أو البريد الإليكترونى مع إستخدام تشفير البيانات عند الضرورة.

وفى سبيل تبادل المعلومات كذلك نصت المادة 26 على إمكانية قيام الدول الأطراف بتبادل المعلومات فيما بينها فى إطار التحقيقات.

أما المادة 27 فقد نظمت الإجراءات المتعلقة بالمساعدة فى حال عدم وجود إتفاقيات تبادل مساعدة.

- **الصورة الثانية: نقل الإجراءات:**

ويقصد به قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة أرتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط معينة[2]، من أبرزها التجريم المزدوج بمعنى أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات.

ولقد أقرت العديد من الإتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، وإتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبرالوطنية 2000م في المادة 21 منها ، وذات الشيء نجده في معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999م في المادة 9 منها ، وأيضا المادة 16 من النموذج الإسترشادي لإتفاقية التعاون القانوني والقضائي

---

(1) اللواء دكتور، محمد فتحى عيد ، المرجع السابق ، ص180.179.

(2) د. سالم محمد سليمان الأوجلي ، المرجع السابق ، ص 427.

الصادر عن مجلس التعاون الخليجي 2003م[1].

وكذلك قيام المجلس الأوروبى بإقرار إتفاقية نقل الإجراءات الجنائية التى تعطى للأطراف المنضمة إمكانية محاكمة الجانى طبقاً لقوانينها ، بناء على طلب دولة أخرى طرف فى هذه الإتفاقية ، بشرط أن يكون معاقباً عليه فى الدولتين[2].

وهناك إتفاقيات دولية على الصعيد العربى موضوعها المساعدة القضائية مثالها الإتفاق العراقى المصرى فى العام 1966 ، والإتفاق اللليبى المصرى فى العام 1992.

- **الصورة الثالثة: الإنابة القضائية الدولية:**

تعرف الإنابة القضائية الدولية بأنها ، طلب من السلطة القضائية المنيبة إلى السلطة المنابة قضائية كانت أم دبلوماسية أساسه التبادل بإتخاذ إجراء من إجراءات التحقيق أو جمع الأدلة فى الخارج وكذا أى إجراء قضائى آخر يلزم إتخاذه للفصل فى المسألة المثارة أو المحتمل إثارتها فى المستقبل أمام القاضى المنيب ليس فى مقدوره القيام به فى نطاق دائرة إختصاصه[3].

وتهدف هذه الصورة إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التى تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى ، كسماع الشهود أو إجراء التفتيش وغيرها[4].

والإنابة القضائية ناتجة عن الواجبات أو الإلتزامات التي يفرضها القانون الدولي العام على الأمم المتحدة مع ضرورة مراعاة إحترام حقوق وحريات الإنسان المعترف بها عالمياً ، ومقابل ذلك تتعهد الدولة الطالبة للمساعدة بالمعاملة بالمثل ، و إحترام النتائج القانونية التي توصلت إليها الدولة المطلوب منها المساعدة القانونية[5].

وقد نصت المادة 19 من إتفاقية التعاون القانونى والقضائى بين دول إتحاد المغرب

---

(1) د.حسين بن سعيد الغافرى ، السياسة الجنائية فى مواجهة جرائم الإنترنت (دراسة مقارنة) ، المرجع السابق ، ص 510 . 511.

(2) د. سليمان أحمد فضل ، المرجع السابق ، ص423.

(3) د. عكاشة محمد عبد العال ، الإنابة القضائية فى نطاق العلاقات الخاصة الدولية ، دار المطبوعات الجامعية ، 1994 ، ص16.

(4) د.حسين بن سعيد الغافرى ، السياسة الجنائية فى مواجهة جرائم الإنترنت (دراسة مقارنة) ، المرجع السابق ، ص511.

(5) د. فائزة يونس الباشا ، الجريمة المنظمة في ظل الإتفاقيات الدولية والقوانين الوطنية ، مرجع سابق ، ص221.

العربى (ليبيا . تونس . الجزائر . المغرب . موريتانيا) والموقعة برأس لانوف بالجماهيرية العظمى عام 1991 ، على الإنابة القضائية حيث نصت على أنه ، (لكل طرف متعاقد أن يطلب إلى أي طرف متعاقد آخر أن يقوم في إقليمه نيابة عنه بأي إجراء قضائي متعلق بدعوى قائمة وبصفة خاصة سماع شهادة الشهود وتلقي تقارير الخبراء ومناقشتهم ، وإجراء المعاينة وطلب تحليف اليمين).

والأمر نفسه هو ما نصت عليه إتفاقية الرياض العربية للتعاون القضائى وذلك فى المادة 14 من الإتفاقية.

ومن الجدير بالذكر أن كل ما سبق ذكره عن التعاون القضائى الدولى والإتفاقيات التى أبرمت بصدده لم تتناول كيفية التعامل القضائى على المستوى الدولى فى حالة إرتكاب جرائم الإنترنت ، الأمر الذى يقتضى إعادة النظر فى هذه الإتفاقيات أو على الأقل تطويع نصوصها لتطبيقها على هذه الجرائم ولو قياساً.

وفى سبيل محاولة تجاوز ذلك أبرمت العديد من الإتفاقيات الجديدة التي ساهمت في تقصير الوقت وإختصار الإجراءات عن طريق الإتصال المباشر بين السلطات المعنية بالتحقيق ، مثال ذلك الإتفاقية الأمريكية الكندية التي تنص على إمكانية تبادل المعلومات شفوياً في حالة الإستعجال[1].

- **الصورة الرابعة: تسليم المجرمين:**

استقر فقه القانون الدولي على إعتبار تسليم المجرمين شكلاً من أشكال التعاون الدولي في مكافحة الجريمة والمجرمين وهذا النوع من التعاون الدولي هو نتيجة طبيعية للتطورات التي حدثت في كافات المجالات ومنها مجال الإتصالات وتقنية المعلومات، حيث لم تعد الحدود القائمة بين الدول تشكل حاجزاً أمام مرتكبي الجرائم كما أن نشاطهم الإجرامي لم يعد قاصرا على إقليم معين بل إمتد إلى أكثر من إقليم ، بحيث بات المجرم منهم يشرع في التحضير لإرتكاب جريمته في بلد معين ويقبل على التنفيذ في بلد آخر ويرتكب الفرار إلى بلد ثالث للإبتعاد عن أيدي أجهزة العدالة . فالجريمة إذاً أصبح لها طابع دولي والمجرم ذاته أصبح مجرما دوليا ، وهذا بالفعل ما ينطبق على الجرائم المتعلقة بالإنترنت[2].

---

(1) د. جميل عبد الباقى الصغير ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت ، دار النهضة العربية ، 1998 ، ص86.

(2) د.حسين بن سعيد الغافرى ، السياسة الجنائية فى مواجهة جرائم الإنترنت (دراسة مقارنة) ، المرجع السابق ، ص513.

ولو أمعنا النظر في نظام تسليم المجرمين لوجدناه يقوم على أساس أن الدولة التي يتواجد على إقليمها المتهم بارتكاب أحد الجرائم العابرة للحدود ومنها الجرائم المتعلقة بالإنترنت عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك ، وإلا كان عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة . فهو إذاً يحقق مصالح الدولتين الأطراف في عملية التسليم ، فهو يحقق مصلحة الدولة الأولى في كونه يضمن معاقبة الفرد الذي أخل بقوانينها وتشريعاتها ، ويحقق في ذات الوقت مصلحة للدولة الثانية المطلوب إليها التسليم كونه يساعدها على تطهير إقليمها من فرد خارج عن القانون ومن شأن بقائه فيها تهديد أمنها واستقرارها[1].

- **تعريف نظام تسليم المجرمين:**

التسليم هو قيام دولة ما (الدولة المطلوب منها التسليم) بتسليم شخص موجود فى أراضيها إلى دولة أخرى (الدولة الطالبة) تبحث عن هذا الشخص إما لمحاكمته لجريمة نسب إليه إرتكابها أو لتنفيذ حكم صدر عن محاكمها بشأنه[2].

ويختلف نظام تسليم المجرمين عن الطرد الذى قد يحدث لأسباب داخلية تخص الدولة التى تصدر أمر الطرد ، وكذلك يختلف عن المنع الذى يتمثل فى الحيلولة دون إجتياز شخص ما حدود الدولة ، ويختلف نظام التسليم كذلك عن الإعادة إلى الوطن التى تقع فى سياق غير جنائى[3].

أما فيما يتعلق بمصادر نظام تسليم المجرمين فلهذا النظام مصدرين إثنين القوانين الوطنية التى غالباً ماتتضمن قواعد وإجراءات وشروط تسليم المجرمين وقواعد القانون الدولى.

وتتعدد فى هذا المجال نصوص القانون الدولى فمنها معاهدات التسليم الثنائية وكذلك إتفاقيات التسليم المتعددة الأطراف مثل إتفاقية التسليم الأوروبية وإتفاقية الكومنولث لتسليم المجرمين الفارين ، وإتفاقية التعاون القضائى لجامعة الدول العربية ، وإتفاقية تسليم المجرمين المبرمة بين الدول الأمريكية ، وإتفاقية التسليم للمجموعة الإقتصادية لدول غرب أفريقيا ، ومعاهدة تسليم المجرمين والمساعدات المتبادلة في المسائل الجنائية الخاصة ببلدان البينولكس، أو الإتفاقيات الدولية التى تتضمن أحكاماً متصلة بقانون التسليم دون أن تكون بحد ذاتها

---

(1) د.حسين بن سعيد الغافرى ، السياسة الجنائية فى مواجهة جرائم الإنترنت (دراسة مقارنة) ، المرجع السابق ، ص514.

(2) تعريف وارد بنشرة الإنتربول الإعلامية المتوافرة بالموقع الإليكترونى
www.interpol.int/Public/ICPO/LegalMaterials/FactSheets/FS11ar.pdf

(3) نشرة الإنتربول الإعلامية سالفة الذكر.

إتفاقيات تسليم[1].

ولعل نظام تسليم المجرمين يتسق ووقع الجرائم المعلوماتية ، ذلك أن هذه الجريمة وكما ذكرنا سلفاً تتسم بالطابع الدولى الذى يسمح بإمكانية إرتكابها فى قطر معين وتحقق نتيجتها فى قطر آخر ، الأمر الذى يجعل نظام التسليم إلى جانب أنواع التعاون القضائى الأخرى أنسب حل للقضاء ولو جزئياً على هذه الظاهرة.

وقد نصت إتفاقية بودابست في المادة 24 على شروط تسليم المجرمين حيث نصت الفقرة الخامسة على خضوع عملية التسليم لقانون الدولة المطلوب منها التسليم ، أو إتفاقيات تسليم المجرمين واجبة التطبيق.

المطلـب الثانـى
الإتفاقيــات والمؤتمــرات الدوليــة

حقيقةً لم تبرم إتفاقيات دولية فى مجال جرائم الإنترنت بالقدر الذى يتلائم أو يتماشى مع إستفحالها ، وتبرز فى هذا السياق إتفاقية بودابست الموقعة فى 2001/11/23 ، بالعاصمة المجرية إضافةً إلى بعض المؤتمرات والملتقيات الدولية التى ناقشت هذه الظاهرة ، وهو ما سنتناوله تباعاً.

أولاً: إتفاقية بودابست لمكافحة جرائم الحاسب الآلى:

لم تكن هذه الإتفاقية وليدة صدفة لدى الدول الأعضاء فيها وإنما سبقتها خطوات تمهيدية عدة وإجتماعات بين هذه الدول لوضع خطوط عريضة يتم على أساسها الوصول لصورة واضحة فى شأن هذه الجرائم ومواجهتها من الناحيتين الموضوعية والإجرائية.

حيث إجتمع في موسكو في عام 1999 وزراء العدل والداخلية للدول الثماني الكبار وطلبوا من ممثليهم وضع خيارات وحلول عملية تسمح بكشف ومتابعة الإتصالات الإليكترونية الدولية في إطار التحقيقات الجنائية ، ثم في عام 2000 وضع الخبراء أيديهم على بداية الحلول والمقترحات التى لاقت بدورها قبولاً لدى رؤساء الدول الثمان الكبار خلال إجتماعهم في أوكيناوا باليابان على بدء الأعمال المقترحة، وفي عام 2001 طالب وزراء العدل والداخلية للدول الثماني الكبار من الخبراء في الإجتماع الذي تم في ميلان، وضع توصيات عن إقتفاء أثر المجرمين على شبكات المعلومات، مع الأخذ في الإعتبار إحترام الحقوق الأساسية مثل حماية المعلومات

(1) نشرة الإنتربول الإعلامية.

الشخصية والحريات الفردية(1).

ثم جاءت أحداث 11 سبتمبر 2001 فجعلت هذا العمل أكثر إلحاحاً وسرعة، إذ أن الإرهابيين يمكنهم إستخدام مواقع الإنترنت والرسائل الإلكترونية وبعض الوسائل التقنية الأخرى في الإتصالات المتطورة، وذلك لعمل مخططاتهم ونشر ونقل المعلومات إلى مختلف القارات، بحيث يصبح كشفها أمراً صعباً إن لم يكن مستحيلاً(2).

وتعد هذه الإتفاقية أول إتفاقية دولية في مجال الجرائم المرتكبة عبر شبكة الإنترنت والشبكات الحاسوبية الأخرى، ومن أهداف هذه الإتفاقية وضع سياسة جنائية مشتركة ضد جرائم الشبكات الحاسوبية. كما ويعتبر الهدف الأساسي للإتفاقية إيجاد إنسجام بين القوانين الجنائية المحلية، وتلتزم الدول الأعضاء في الإتفاقية بالعمل على وضع قانون جنائي إجرائي محلي يُيَسر التحقيق والملاحقة القضائية للمخالفات التي ترتكب بواسطة أجهزة الحاسب الآلى ، بالإضافة إلى إيجاد تصور لنظام تعاون دولي فعال لمحاربة مثل هذه الجرائم.

وقد تم إقتراح نصوص الإتفاقية من خلال هيئة شكلت خصيصاً لهذه الغاية، سميت بـ "لجنة الخبراء في الجرائم الواقعة في الشبكات الحاسوبية" ، وتتألف هذه اللجنة من خبراء ليس فقط من الدول الأعضاء في مجلس أوروبا بل أيضاً من دول أخرى مثل الولايات المتحدة وكندا واليابان وغيرها.

وبناءً على ما تقدم فإن المجال مفتوح للتوقيع على هذه الإتفاقية أمام الدول الأعضاء في مجلس أوروبا والدول غير الأعضاء التي شاركت في وضع مسودة الإتفاقية. كما يجوز للدول غير الأعضاء الأخرى الإنضمام إن إتفقت كل الدول الأعضاء على دعوتها.

وقد تم تنظيم المعاهدة كما يلي:

- **الفصل الأول** : تعريفات بنظام الكمبيوتر، وبيانات الكمبيوتر، ومقدم الخدمة، وبيانات الحركة عبر شبكات الاتصال.
- **الفصل الثاني** : التدابير التي يجب اتخاذها على المستوى الوطني. وتنقسم إلى:

– **القسم الأول** : القانون الجنائي الموضوعي، عن السلوكيات التي يجب اعتبارها جريمة جنائية.

– **القسم الثانى** : قانون الإجراءات، ويتناول التدابير التي تتخذ لإجراء تحقيقات أكثر فعالية

(1) د. صالح أحمد البربري ، المرجع السابق ، ص14. 15.

(2) د. صالح أحمد البربري ، المرجع السابق، ص15.

فيما يتعلق بجرائم الإنترنت، ويجب التأكيد على أن هذه التدابير الإجرائية يمكن استخدامها مع أية جرائم جنائية يشترك فيها نظام للكمبيوتر .على سبيل المثال، يمكن إستخدامها في حالة الإرهاب، أو غسيل الأموال، أو الاتجار بالبشر، أو الفساد أو غيرها من الجرائم الخطيرة التي تستخدم فيها تكنولوجيا المعلومات والاتصالات.

- **القسم الثالث** : الاختصاص القضائي.

- **الفصل الثالث** : التعاون الدولي. وينقسم هذا الفصل إلى:

- **القسم الأول** : المبادئ العامة للتعاون، وهي المبادئ العامة للتعاون الدولي، والمبادئ المتعلقة بتسليم المجرمين، والمبادئ المتعلقة بالمساعدات القانونية المتبادلة، والمعلومات المقدمة طواعية، والمساعدة القانونية المتبادلة في حال عدم وجود وثائق دولية معمول بها، والسرية ووضع حد للإستخدام.

وقبل توقيع تلك الإتفاقية كانت هناك إجراءات للتعاون القضائي التقليدي الذي يتم بسرعة للحصول على المعلومات التاريخية في نفس الوقت تقريبا، خصوصاً عندما يتعلق الأمر ببلدين فقط (بمعنى بلد الضحية وبلد مرتكب الجريمة) إلا أنه عندما يقوم الجاني بتمرير إتصالاته عبر ثلاث أو أربع أو خمس دول فإن إجراءات التعاون القضائي تستغرق كثيراً من الوقت قبل أن يحصل رجال الشرطة على المعلومات الخاصة بمؤدي خدمة لكي يصلوا إلى مصدر الجريمة، وهو ما يزيد من مخاطر عدم إمكانية الوصول إليه وفقدان المعلومات، وعلى ذلك يظل المجرم مجهولاً طليقاً يمارس أنشطته الإجرامية، لذلك أعلن الاسترالي ديز بيرويك المدير العام لمركز بحوث الشرطة الاسترالي أن الجريمة الإلكترونية تستخدم شبكة دولية ومن الضروري أن تتم التحقيقات بطريقة مشابهة في العالم أجمع[1].

- **القسم الثانى** : أحكام خاصة لتحقيق المزيد من التعاون الفعال، ويسمح ذلك للأطراف المنضمة للاتفاقية بتطبيق الأدوات الإجرائية على المستوى الدولي أيضا، كما ينص هذا القسم أيضا على تكوين شبكة من الجهات التي يمكن الاتصال بها المتاحة طوال أيام الأسبوع على مدار أربع وعشرين ساعة لتسهيل التعاون السريع.

- **الفصل الرابع** : الأحكام الختامية، ويهتم هذا الفصل على وجه الخصوص بالدول غير الأوروبية كما ينص على سبل إنضمام الدول غير الأعضاء إلى الإتفاقية.

---

(1) د. صالح أحمد البربري ، المرجع السابق ، ص19.

ويبرز دور إتفاقية مكافحة جرائم الإنترنت فى إطار التعاون الدولى وذلك فى عدة نقاط:

. تعمل الإتفاقية على ضمان تناسق وتوافق أحكام القانون الجنائي بشأن جرائم الإنترنت بين البلدان.

. تقدم الإتفاقية أدوات لجمع الأدلة الإلكترونية، وأدوات للتحقيق في غسيل الأموال عبر الإنترنت، والإرهاب بواسطة الإنترنت، وغيرها من الجرائم الخطيرة، ومن خلال الإتفاقية يمكن تطبيق تلك الأدوات في إطار التعاون الدولي.

. نصت الإتفاقية على الأسس القانونية لتطبيق القانون الدولي والتعاون القضائي مع الأطراف الأخرى في الإتفاقية.

. الإتفاقية متاحة لأية دولة ترغب في الانضمام إليها.

وقد ألحق بالإتفاقية البروتوكول الإضافي الموقع فى ستراسبورغ 28 يناير 2003 ، والذي أضاف بدوره إلى أحكام المعاهدة أحكام تتعلق بتجريم أعمال العنصرية وكره الأجانب المرتكبة عبر أنظمة الحاسوب.

ثانياً: إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية:

والتي تم التوقيع عليها في مدينة باليرمو عام 2000 ، وتهدف في المقام الأول إلى تطوير التعاون بين الدول، وقد نصت على مكافحة الجريمة المنظمة عبر الوطنية التي ترتكب بإستخدام الحواسيب أو شبكات الإتصالات السلكية واللاسلكية أو غير ذلك من أشكال التكنولوجيا الحديثة وتحتوي الإتفاقية على أشكال مختلفة من التعاون الدولي في مجال المساعدة القانونية المتبادلة و تسليم المجرمين، التحقيقات المشتركة ونقل الإجراءات الجنائية كما تدعو الإتفاقية جميع الدول إلى عقد إتفاقيات أخرى بهدف تعزيز هذا التعاون.

ثالثاً: قرار الجمعية العامة للأمم المتحدة لمكافحة إستغلال تكنولوجيا المعلومات لأهداف إجرامية(1):

يحث هذا القرار الدول الأعضاء على تنسيق أعمال أجهزة الردع لديها وتبادل المعلومات بشأن المشكلات التي تواجههم في مكافحة إستغلال تكنولوجيا المعلومات لتحقيق أهداف إجرامية، ويؤكد القرار أن أنظمة المساعدة القانونية المتبادلة تُمكِّن من إجراء تحقيقات بشكل سريع في قضايا

---

(1) القرار رقم 55/63 للجمعية العامة للأمم المتحدة الذى تم تبنيه بتاريخ 4 ديسمبر 2000 ، يمكنك الإطلاع عليه من خلال الموقع التالي:

http://www.cybersecuritycooperation.org/moredocuments/International%20Agreements/55-63%20French.pdf

إستغلال تكنولوجيا المعلومات لأهداف غير مشروعة وتحّث على الجمع والتبادل السريع لعناصر الأدلة المتعلقة بهذه القضايا.

رابعاً : مقررات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكمبيوتر(1):

عقد هذا المؤتمر فى ريو دي جانيرو بالبرازيل فى الفترة من 4–9 أكتوبر 1994، وقد تناول المؤتمر الجانب الموضوعى والإجرائى لهذه الجرائم على النحو التالى:

البند الأول : الشق الموضوعي(الجرائم).

إعتبر المؤتمر الأفعال الآتية من قبل جرائم الكمبيوتر والإنترنت.

1. **الإحتيال أو الغش المرتبط بالكمبيوتر:** ويشمل الإدخال والإتلاف والمحو لمعطيات الكمبيوتر أو برامجه وذلك بقصد جني الفاعل منافع اقتصادية له أو للغير.
2. **تزوير الكمبيوتر أو التزوير المعلوماتي:** وذلك بإرتكاب أفعال التزوير المنصوص عليها فى قانون العقوبات الوطنى لكل دولة.
3. **الإضرار بالبيانات والبرامج** :(الإتلاف).
4. **الدخول غير المصرح به:** وهو الولوج دون تصريح إلى نظام معلوماتى عن طريق إنتهاك إجراءات الأمن.

البند الثاني: الشق الإجرائي.

أما القواعد الإجرائية فقد تناولها المؤتمر على النحو التالى:

1– يتطلب التنقيب بالنسبة لجرائم الحاسب الآلي أن نضع تحت تصرف سلطات التحقيق والتحري إمكانات كافية تتعادل مع الحماية الكافية لحقوق الإنسان وحرمة الحياة الخاصة .

2. على ضوء هذه المبادئ العامة يجب أن يحدد بوضوح ما يلي:

أ. السلطات التي تقوم بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات ، وخاصة ضبط الأشياء غير المحسوسة وتفتيش شبكات الحاسوب .

ب . واجبات التعاون الفعال من جانب المجني عليهم، والشهود، وغيرهم من مستخدمي تكنولوجيا المعلومات، فيما خلا المشتبه فيه (خاصة لكي تكون المعلومات متاحة في صورة يمكن إستخدامها للأغراض القضائية).

---

(1) راجع بخصوص هذا المؤتمر الموقع التالى:
http://www.f-law.net/law/showthread.php?10802

ج . السماح للسلطات العامة باعتراض الاتصالات داخل نظام الحاسوب ذاته ، أو بينة وبين نظم الحاسبات الأخرى . مع إستخدام الأدلة التي يتم الحصول عليها في الإجراءات أمام المحاكم .

3. نظرا لتعدد وتنوع البيانات المدرجة في نظم معالجة البيانات ، فان تنفيذ المكنات القسرية (المنوطه برجال السلطة العامة) يجب أن يكون متناسباً مع الطابع الخطير للإنتهاك ، ولا يسبب سوى الحد الأدنى من إعاقة الأنشطة القانونية للفرد . كما يجب عند بدء التحريات أن يوضع في الإعتبار كل القيم المرتبطة ببيئة تكنولوجيا المعلومات ، مثل ضياع فرصة اقتصادية ، إنتهاك حرمة الحياة الخاصة ، مخاطر الخسارة الاقتصادية ، كلفة إعادة بناء تكامل البيانات كما كانت من قبل .

4– القواعد القائمة في مجال قبول ومصداقية الأدلة ، يمكن أن تثير مشاكل عند تطبيقها ، نظرا لتقييم تسجيلات الحاسبات في الإجراءات القضائية لذا ينبغي إدخال بعض التغييرات التشريعية في حالة الضرورة.

خامساً: القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء ـ هافانا 1990 ـ بشأن الجرائم ذات الصلة بالكمبيوتر(1).

وضع المؤتمر المنعقد من قبل الامم المتحدة والمعنى بمنع الجريمة ومعاملة السجناء عدة توصيات فيما يتعلق بجرائم الإنترنت تمثلت فى:

1. يهيب المؤتمر بالدول الأعضاء ، في ضوء الأعمال المطلع بها فعلا في مجال الجرائم ذات الصلة بالكمبيوتر أن تكثف جهودها كي تكافح بمزيد من الفعالية عمليات إساءة إستعمال الكمبيوتر التي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني بما في ذلك النظر ، إذا دعت الضرورة إلى ذلك ، في التدابير التالية :–

أ . تحديث القوانين وأغراضها الجنائية فيما يتعلق بالتجريم والعقاب وإجراءات التحقيق ، وقواعد الإثبات ، والمصادرة ، والمساعدة القانونية المتبادلة وتسليم المجرمين من أجل:

. ضمان أن تطبق الجزاءات والقوانين الراهنة، بشأن سلطات التحقيق وقبول الأدلة في الإجراءات القضائية على نحو ملائم وإدخال تغييرات مناسبة إذا دعت الضرورة إلى ذلك.

---

(1) راجع بهذا الخصوص الموقع : http://www.f-law.net/law/showthread.php?10801

. وضع أحكام وإجراءات تتعلق بالتحقيق والأدلة للتصدي إلى هذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي.

. مصادرة أو رد الأصول بصورة غير مشروعة والناجمة عن إرتكاب جرائم ذات صلة بالحاسوب.

ب . تحسين تدابير الأمن والوقاية المتعلقة بالحاسوب مع مراعاة حماية الخصوصية وإحترام حقوق الانسان وحرياته الأساسية.

ج . إعتماد تدابير لزيادة وعي الجماهير والعاملين في الأجهزة القضائية وأجهزة انفاذ القوانين بالمشكلة وبأهمية مكافحة الجرائم ذات الصلة بالحواسيب.

د . إعتماد تدابير مناسبة لتدريب القضاة والمسؤولين والأجهزة المسؤولة عن منع الجرائم الإقتصادية والجرائم ذات الصلة بأجهزة الحاسوب والتحقيق فيها ومحاكمة مرتكبيها وإصدار الأحكام المتعلقة بها.

هـ . التعاون مع المنظمات المهتمة بهذا الموضوع في وضع قواعد للآداب المتبعة في إستخدام أجهزة الحاسوب وتدريس هذه الآداب ضمن المناهج الدراسية.

و. إعتماد سياسات بشان ضحايا الجرائم المتعلقة بالكمبيوتر تنسجم مع إعلان الأمم المتحدة بشأن مباديء العدل المتعلقة بضحايا الإجرام والتعسف في إستعمال السلطة ، وتتضمن إعادة الممتلكات التي يتم الحصول عليها بطرق غير مشروعة ، وتدابير لتشجيع الضحايا على إبلاغ السلطات المختصة بهذه الجرائم.

2. الإهتمام بمعاملة ضحايا الجرائم ذات الصلة بالحواسيب وتشجيعهم على الإبلاغ عن هذه الجرائم.

3. وضع صك دولى يتناول حوسبة نظم العدالة الجنائية من أجل زيادة فعالية إدارة عمليات إدارة العدالة الجنائية ونظم المعلومات.

والجدير بالذكر أن مؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين المنعقد فى القاهرة عام 1995 ، قد ركز على الجرائم ذات الصلة بالحاسب الآلى ، وتأكد التركيز على تلك الجرائم فى المؤتمر العاشر المنعقد فى فيينا عام 2000.

ولقد أوصى المؤتمر المنعقد فى فيينا بعدد من التوصيات الهامة فى هذا الصدد وذلك

على النحو التالى[1]:

1. أن تقوم الدول . إذلم تكن قد فعلت . بتجريم الأفعال ذات الصلة بالحواسيب والتى ينبغى تأثيمها.
2. أن تقوم الدول بإصدار قوانين إجرائية ملائمة للتحقيق فى جرائم الحاسوب وملاحقة مجرمى الإنترنت.
3. أن تعمل الحكومات مع المسئولين فى صناعة الحاسوب والإنترنت فى تعاون وثيق شفاف لمنع الجرائم الحاسوبية ومكافحتها حتى يصبح الإنترنت مجالاً آمناً مع مراعاة الدوافع التجارية للقطاع الخاص وإهتمامه بالناحية التقنية لا القانونية.
4. تحسين التعاون الدولى من أجل إقتفاء أثر المجرمين على الإنترنت.
5. أن تعمل الأمم المتحدة على توفير العون والمساعدة التقنية للدول التى تطلبها بشأن الجرائم ذات الصلة بالشبكة الحاسوبية.

سادساً: أجندة تونس[2].

تم صياغة بنود هذه الأجندة بتاريخ 15 نوفمبر 2005 خلال القمة العالمية لمجتمع المعلومات تحت رعاية الأمم المتحدة والتي وضعت عدداً من التوصيات تمثل فى:

. أهمية ملاحقة مرتكبي جرائم الإنترنت، بما في ذلك الجرائم المرتكبة في إحدى الدول لكن تأثيرها يتعدى إلى دولة أخرى.

. ضرورة إمتلاك الوسائل والآليات الفعالة على المستوى الوطني والدولي من أجل تعزيز التعاون الدولي، بما في ذلك قوات الشرطة وسلطات القضاء في مجال مكافحة جرائم الإنترنت.

. حث الدول على مشاركة جميع الأطراف المعنية لصياغة التشريع الضروري والذي يسمح بإجراء تحقيقات في جرائم الإنترنت والملاحقة القضائية لمرتكبي هذه الإعتداءات أخذا بعين الإعتبار الأطر القضائية الموجودة.

---

(1) راجع فى ذلك ، اللواء دكتور ، محمد فتحى عيد ، مرجع سابق ، ص183.

(2) عنوان الوثيقة Tunis Agenda For The Information Society ، يمكنك الإطلاع على محتوى الوثيقة من خلال الموقع الإليكترونى http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

سابعاً: المؤتمر الدولي الأول لحقوق الإنسان الخاص بأثر التقدم التكنولوجي على حقوق الإنسان(مؤتمر طهران 1968).

تبنت الجمعية العامة للأمم المتحدة توصيات هذا المؤتمر حيث تم الإعتراف بالحق فى الخصوصية ، وبناءً على هذه التوصيات سنت بعض دول العالم في أوربا وآسيا وأمريكا واليابان تشريعاتها في مجال حماية الخصوصية من الإعتداء عليها ألزمت من خلالها مواقع الإنترنت المعنية بجمع المعلومات بتسجيل أغراضها وإخضاع عملياتها لرقابة الدولة.

المطلــب الثالــث

معوقـــات التعـــاون الدولـــى

يواجه التعاون الدولى فى مواجهة جرائم الإنترنت عدة معوقات وصعوبات تتمثل فى:

أولاً - الإختصـــاص:

ذكرنا فى أكثر من مناسبة فى هذا البحث أن جرائم الإنترنت تتميز بالطابع الدولى العابر للحدود ، وهو ما يصعب من إمكانية تطبيق نصوص قانون العقوبات الوطنية والتى تتميز بخصيصة الإقليمية ، أى سريان القانون العقابى ونصوصه على الأفعال المرتكبة داخل القطر أو الدولة فقط ، وعدم تعديها لأى أفعال إجرامية ترتكب خارجها إلا فى أحوال إستثنائية وفى أضيق الحدود.

وفى جرائم الإنترنت فإن الفعل الإجرامى قد يرتكب فى دولة ما ولكن النتيجة المترتبة عليه قد تتعدى الحدود الإقليمية لدولة أو ربما دول أخرى ، فالطابع العالمي لتكنولوجيا المعلومات يمكن أن يكون النشاط الإجرامي حقًا عبر الوطنية، فالشخص الذي يجلس في أسبانيا يمكنه أن تعطيل جهاز كمبيوتر في سنغافورة ، أو نشر المواد الإباحية عن الأطفال في سوازيلاند، وهذه المشاكل تصعب من ممارسة السيادة الوطنية على تدفقات والمعلومات والمسائل المتعلقة بالولاية القضائية(1)، والأهم من ذلك أن مختلف البلدان لديها قوانين مختلفة ، وتتفاوت فيما بينها فى تعريف الجرائم والعقوبات إضافةً إلى حواجز اللغة(2).

---

(1) Dr. Peter Grabosky, Crime And Technology In The Global Village, Paper Presented at: The Conference: Internet Crime, held in Melbourne, 16-17 February 1998, by the Australian Institute of Criminology,p4.

(2) Raphael F.Perl , Terrorist Use of the Internet Threat, Issues, and Options for International Co-operation , Second International Forum on Information Security, Garmisch-Partenkirchen, 7-10 April 2008, p3.

وهو ما يدعو إلى التساؤل عن المكان المعتبر قانوناً لوقوع الجريمة في هذه الحالة ، فهل هو مكان وقوع الفعل الإجرامي أم المكان الذي تحققت فيه النتيجة ؟ ومن الدولة صاحبة الإختصاص بنظر الدعوى المترتبة على جرائم الإنترنت ، هل هى الدولة التى أرتكب داخلها الفعل ، أم الدولة التى تحققت فيها نتيجة هذا الفعل؟

وللإجابة على هذا التساؤل إنقسم الفقه إلى ثلاثة إتجاهات ، فذهب الإتجاه الأول إلى أن العبرة في تحديد مكان وقوع الجريمة بالمكان الذي وقع فيه الفعل بغض النظر عن المكان الذي تحققت فيه النتيجة ، وذهب إتجاه آخر إلى أن مكان وقوع الجريمة يتحدد بالمكان الذي تحققت فيه النتيجة أو كان من المفترض تحققها فيه ، وذهب إتجاه ثالث إلى أن العبرة في ذلك تكون بمكان حصول أي منهما (السلوك أو النتيجة). وفيما يلى عرض لكل مذهب وما استن إليه من أسانيد وحجج.

1 ـ مذهب الفعل أو النشاط الإجرامي بوصفه معياراً لتحديد مكان وقوع الجريمة:

وفقاً لهذا المعيار ينعقد الإختصاص للمحكمة التي يقع في نطاقها النشاط الإجرامي وليس مكان حصول النتيجة أو الآثار المترتبة عليه ، بدعوى أن إتخاذ آثار الفعل كمناط لتحديد مكان وقوع الجريمة تكتنفه بعض الصعوبات يمكن إجمالها في أنه معيار مرن وفضفاض ، فضلاً عن أن معيار حصول النشاط أدعى إلى تيسير عملية الإثبات وجمع أدلة الجريمة ، وأن المحكمة التي لها ولاية نظر الدعوى تكون قريبة من مسرح الجريمة ناهيك أن الحكم الذي يصدر في الواقعة يكون أكثر فعالية ويسهل معه ملاحقة الجناة[1].

وقد حظي هذا الإتجاه بتأييد جانب كبير من الفقه سواء في فرنسا أو مصر ، ليس هذا فحسب ، بل اتجهت بعض التشريعات المقارنة إلى تبنيه ، ومن هذا القبيل القانون الدولي الخاص النمساوي الصادر سنة 1979 والمجري الصادر في السنة ذاتها[2].

ويضيف المؤيدون لهذا الإتجاه حججاً أخرى ، منها أن حدوث الضرر في مكان معين مردّه في الغالب أسباب لا إرادة لمقترف السلوك فيها ، وأن من شأن تطبيق قانون الدولة التي تحقق في نطاقها الضرر لا يتفق وإعتبارات العدالة نظراً لجهل الجاني بهذا القانون الذي يتم إعماله بحقه ، وفي الغالب ليس ممكناً العلم به إذ حينما أقدم على ارتكاب الفعل الذي أتاه يعتقد مشروعيته وفقاً لقانون البلد الذي وقع فيه السلوك ، وإذا به غير ذلك من منظور قانون البلد الذي

(1) راجع بهذا الخصوص د. أحمد عبد الكريم سلامة ، قانون حماية البيئة ، دراسة تأصيلية في الأنظمة الوطنية والإتفاقية ، الطبعة الأولى ، منشورات جامعة الملك سعود ، السعودية ، 1997 ، ص535.

(2) د. أحمد عبد الكريم سلامة ، المرجع السابق ، ص588.

تحقق فيه الضرر [1].

وقد تعرض هذا الإتجاه للنقد وذلك بسبب تركيزه على مكان إرتكاب الجريمة فقط وإهماله المكان المحققة فيه نتيجة هذا الفعل.

2 ـ مذهب مكان تحقق النتيجة كمعيار لوقوع الجريمة:

يذهب هذا الإتجاه إلى أن المكان الذى تتحقق فيه نتيجة الفعل الإجرامى هو المكان الذى ينعقد لمحكمته الإختصاص بنظر الدعوى الناشئة عن الجريمة، ذلك أن وقع الجريمة لا يكون إلاّ في المكان الذي ظهرت فيه آثارها الضارة التي كان الجانى يرغب في تحقيقها، حيث أن مكان وقوع السلوك لا يعدو أن يكون مصدر الضرر ليس إلاّ.

ومن المبررات التي سيقت لتعزيز هذا الإتجاه أن الأخذ به يحقق وحدة الجريمة وعدم الفصل بين عناصرها ، كذلك يمتاز هذا الإتجاه في نظر المدافعين عنه بأنه أكثر واقعية على إعتبار أن الضرر له مظهر خارجي ملموس خلافاً للنشاط الذي قد لا يكون كذلك متى ما اتخذ صورة الإمتناع أو السلوك السلبي ، وقد لقي هذا الإتجاه ترحيباً من بعض الفقه إلى جانب ذلك تم تبنيه من بعض التشريعات المقارنة ، ومنها القانون الألماني الصادر في 5 ديسمبر 1975 ، والقانون الدولي الخاص التركي الصادر سنة 1982[2].

وقد أخذ القضاء الأمريكي بهذا الإتجاه ، ومن أبرز الأمثلة على ذلك الواقعة التى قدم فيها شخص يحمل الجنسية الإنجليزية إلى المحاكمة أمام إحدى محاكم ولاية ماسوشيتس الأمريكية عن تهمة القتل العمدي والتي قضت بإختصاصها بنظر الدعوى عن الواقعة المذكورة ، على الرغم من أن النشاط حصل على متن مركب إنجليزي في عرض البحر في حين أن وفاة المجني عليه جراء هذا الفعل تمت إثر وصوله إلى الولاية المذكورة[3].

ومع ذلك فإن هذا الإتجاه لم يسلم هو الآخر من النقد ، الذي يتركز في أن الأخذ به يفضي في نهاية المطاف إلى عدم تجريم الشروع إذا لم تتحقق النتيجة الإجرامية.

3 ـ المذهب المختلط:

أمام الإنتقادات التي تعرض لها كلا الإتجاهين السابقين ، برز إتجاه ثالث مفاده أن الجريمة تعد واقعة في مكان حصول النشاط (العمل التنفيذي) ، وكذلك المكان الذي تحققت فيه النتيجة أو الذي من المتوقع أو من المنتظر تحققها فيه.

---

(1) د.موسى مسعود ارحومة ، المرجع السابق ، ص15.

(2) د.موسى مسعود ارحومة ، المرجع السابق ، ص16.

(3) د. أحمد عبدالكريم سلامة ، المرجع السابق ، ص588.

وقد حظي هذا الإتجاه بمباركة أغلب الفقه ، ويجد مبرره في أن الركن المادي للجريمة يقوم على ثلاثة عناصر وهي الفعل (النشاط) والنتيجة وعلاقة السببية ، ما يعني أن الجريمة تعد واقعة في كل مكان تحقق فيه عنصر من عناصر الركن المادي ، أي في مكان النشاط ومكان النتيجة على حد سواء[1].

وبناءً على ذلك يتم تغليب قانون المكان الذى تحققت فيه النتيجة إذا كانت الجريمة تامة ومن قبيل ذلك جرائم السلوك والنتيجة (الجرائم المادية) ، في حين يطبق قانون مكان النشاط أو السلوك إذا كانت الجريمة قد وقفت عند حد الشروع أو كانت من قبيل جرائم السلوك المجرد.

وبعد أن عرضنا للمذاهب الثلاثة فيما يتعلق بالقانون الواجب التطبيق فى حالة تعدى الجريمة الحدود الدولية لأكثر من دولة ، فإنه ووفقاً للمنطق فإن الإتجاه الأخير (المختلط) هو الأجدر بالتأييد سيما فى الجرائم المتعلقة بالإنترنت ، فهذه الجرائم قد ترتكب فى دولة وتتحقق نتيجتها فى دولة أخرى ، وبالتالى فإن الإختصاص بمحاكمة الجانى فى هذه الحالة من الممكن أن يكون للدولة التى صدر فيها الفعل الإجرامى وكذلك من الممكن أن يكون للدولة التى تحققت على أراضيها نتيجة هذا الفعل.

وعلة ذلك أن الأخذ بمذهب السلوك معناه إنعدام الإختصاص القضائى للدولة المتحققة فيها نتيجة الفعل الإجرامى ، ومعناه أيضاً إمكانية عدم قيام الدولة التى وقع فيها السلوك بمحاكمة الجانى بحجة أن لا ضرر وقع فى نطاق إختصاصها ، ونفس الأمر ينطبق على مذهب مكان تحقق النتيجة ، أما المذهب المختلط فيتميز بالمرونة التى توسع من نطاق الحماية الجنائية للجرائم ذات الأبعاد الدولية.

وقد تصدت إتفاقية بودابست لمشكلة الإختصاص وذلك فى المادة 22 التى نصت 22 على أن : " لكل طرف إتخاذ الإجراءات التشريعية وغيرها التي يراها لازمة لكي يحدد اختصاصه بالنسبة لكل جريمة تقع وفقاً لما هو وارد في المواد من 2 إلى 11 من الاتفاقية الحالية عندما تقع الجريمة:

1. أ – داخل النطاق المحلي للدولة :

ب– على ظهر سفينة تحمل علم تلك الدولة.

ج– على متن طائرة مسجلة في هذه الدولة.

د– بواسطة أحد رعاياها، إذا كانت الجريمة معاقباً عليها جنائياً في المكان الذي ارتكبت فيه

(1) د.موسى مسعود ارحومة ، المرجع السابق ، ص20 ـ 21.

أو إذا كانت الجريمة لا تدخل في أي اختصاص مكاني لأي دولة أخرى.

2. ولكل طرف أن يحتفظ لنفسه بالحق في عدم تطبيق، أو عدم التطبيق إلا في حالات وفي ظل شروط خاصة، قواعد الإختصاص المنصوص عليها في الفقرة الأولى (ب و د) من هذه المادة أو في أي جزء من هذه الفقرات.

3. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لإقرار الإختصاص القضائى بشأن الجرائم المشار إليها فى المادة 24 فقرة 1 من هذه الإتفاقية ، فى الحالات التى يكون فيها الجانى المزعوم موجوداً فى إقليمه، ولا يقوم بتسليمه لطرف آخر وذلك بعد طلب التسليم.

4. لا تستبعد هذه الإتفاقية أى إختصاص جنائى يمارسه أح الأطراف وفقاً لقانونه الوطنى.

5. فى حالة مطالبة أكثر من طرف من الأطراف بالإختصاص القضائى بشأن جريمة ما تقرها هذه الإتفاقية ، يقوم الأطراف المعنيون متى كان ذلك ملائماً ، بالتشاور بغرض تحديد الإختصاص القضائى الأكثر ملائمة للمحاكمة.

ثانياً: إختلاف صورالنشاط الإجرامى ما بين دولة وأخرى:

ذلك أن الأنظمة القانونية في بلدان العالم قاطبة لم تتفق على صور محددة يندرج في إطارها ما يسمى بإساءة إستخدام نظم المعلومات الواجب إتباعها ، كذلك ليس هناك تعريف محدد للنشاط المفروض أن يتفق على تجريمه، وذلك نتاج طبيعي لقصور التشريع ذاته في كافة بلدان العالم وعدم مسايرته لسرعة التقدم المعلوماتي.

ثالثاً: عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة:

خاصة ما تعلق منها بأعمال الإستدلال أو التحقيق، سيما وأن عملية الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة، عن طريق الضبط أو التفتيش في نظام معلوماتي معين هو أمر غاية في الصعوبة، فضلاً عن الصعوبة الفنية في الحصول على الدليل ذاته.

رابعاًً: عدم وجود معاهدات ثنائية أو جماعية بين الدول:

من معوقات التعاون الدولى كذلك ، عدم وجود معاهدات ثنائية أو جماعية بين الدول على نحو يسمح بالتعاون المثمر في مجال هذه الجرائم، وحتى في حال وجودها فإن هذه المعاهدات قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم برامج الحاسب وشبكة الإنترنت، ومن ثم يظهر الأثر السلبي في التعاون الدولي.

الخاتمـــــة

الآن وبعد أن إنتهينا من دراسة موضوعنا ، فإنه من الضرورى إبراز أهم ما توصل إليه البحث من نتائج إضافةً إلى التوصيات المقترحة لسد النقص أو القصور فى كيفية مواجهة هذه الجريمة.

- **ولنبدأ أولاً بالنتائج التى توصل إليها البحث:**

1. جريمة الإنترنت جريمة كأى جريمة أخرى عادية ، من حيث وجود جانى ومجنى عليه وركن مادى وآخر معنوى إضافةً للقصد جنائى ، ولكن أهم ما يميزها عن الجرائم الأخرى هو أسلوب إرتكابها ، الذى يتسم بالحداثة فالشرطة فى جريمة من الجرائم قد تحرز سلاحاً أبيض استعمله الجانى أو مسدساً ، أما الجريمة محل البحث فإن أداة إرتكابها هى شاشة الكمبيوتر ولوحة المفاتيح والفأرة ، وكذلك تتميز هذه الأدوات سالفة الذكر عن أى سلاح آخر مستخدم فى الجرائم الأخرى بأنها متاحة للكافة ولا تحتاج لترخيص أو إذن مسبق بإقتنائها.
2. مجرم الإنترنت كذلك يتميز عن باقى المجرمين العاديين ، فبينما يمتاز المجرم العادى بإختلافه عن غيره من الناس من حيث المظهر الخارجى والسلوكى والعقلى أو التعليمى ومن حيث حتى مظهره وكيف يبدو ، نجد على الجانب الآخر مجرم الإنترنت شخص عادى لا يشذ عن أقرانه من الناس من حيث الصفات التى ذكرناها ، ولكن أهم ما يميزه عن المجرم العادى هو أنه فى جريمته يعتمد على عقله وذكائه وثقافته فقط دون اللجوء لإستخدام القوة.
3. تتميز جريمة الإنترنت بالطابع العالمى ، فهى لا تعترف بحواجز الزمان ولا المكان ولا حتى بالحدود الإقليمية للدول.
4. جرائم الإنترنت صعبة الإثبات، حيث أنها لا تترك أثر لها لقيام الجناة بمحو ما يدل عليها بعد إرتكابها حتى وإن وجدت هذه الآثار فمن السهل تدميرها.
5. إفتقار القوانين العقابية فى الكثير من البلدان لنصوص رادعة خاصة بهذه الجرائم.
6. ونتيجة لعدم وجود نصوص قانونية تجرم هذه الأفعال ، فإن أغلب الدول تلجأ لتطبيق النصوص التقليدية وتطويعها فى مواجهة جرائم الإنترنت وكأنها هى الدواء الشافى من هذا الداء ، حيث نجد أن أغلب الدول العربية على وجه التحديد لم تشرع فى سن أى قوانين أو ضوابط خاصة بهذه الجريمة بإستثناء بعض الدول التى حاولت ، وقد ذكرنا فى بحثنا نظام

مكافحة جرائم المعلوماتية فى المملكة العربية السعودية والذى يعتبر خطوة سباقة فى هذا المجال، وكذلك قانون التوقيع الإليكترونى فى مصر.

7. الجهل المعلوماتى لدى جهات التحقيق لقيامها بإتباع الإجراءات التقليدية التى تفتقر إلى الجدوى فى مثل هذه الظروف ، فيما يتعلق بعمليات الإستدلال والتحقيق وعمل التحريات والمعاينات والتفتيش، الأمر الذى يؤدى لإفلات الجناة لصعوبة الحصول على دلائل إدانتهم.

8. رأينا فى بحثنا أن الدول المتقدمة وعلى رأسها أمريكا إبتكرت نظام تلقى الشكاوى والبلاغات مباشرة على شبكة الإنترنت دون الحاجة للإبلاغ عن وقوع مثل هذه الجرائم بالطرق العادية ، وهو ما يوفر الكثير من الوقت والجهد.

9. هناك وسائل عدة للتأمين والحماية من الإعتداءات التى قد تقع عن طريق الإنترنت ، ولكن وبرغم ذلك يبتكر الجناة أساليب جديدة وحديثة لخرق وسائل الحماية.

10. إستحداث بعض الدول لإدارات شرطية جديدة أو ما يسمى شرطة الإنترنت.

11. جريمة الإنترنت لاقت إهتماماً دولياً واسع المدى من قبل دول الإتحاد الأوروبى تجسد فى إتفاقية بودابست ، وكذلك تصدرت هذه الجريمة جدول أعمال الأمم المتحدة فى عديد المناسبات.

- **أما بخصوص التوصيات فقد إرتأينا التالى:**

1. ضرورة العمل على وضع تشريعات خاصه بإستخدام شبكة الإنترنت وبيان الجرائم المرتكبة من خلالها، وتحديد عقوباتها ما بين حدين أدنى وأقصى كما هو الحال فى باقى الجرائم.

2. ولحين صدور تشريعات خاصة بالإنترنت ينبغى تعديل نصوص قانون العقوبات بالإضافة بحيث تنص صراحة على هذه الجرائم.

3. تأهيل المختصين بالتحقيق فى جرائم الإنترنت ، وكيفية إثبات تلك الجرائم وضبط الأدلة المتحصلة منها والأهم من ذلك ضبط الجناه.

4. إنشاء وحدات وإدارات شرطية خاصة بمكافحة جرائم الإنترنت.

5. العمل على إبرام مزيد من الإتفاقيات الدولية فى هذا المجال ، وتفعيل التعاون الدولى فى مجال المساعدات القضائية وتبادل المعلومات وتسليم المجرمين المتهمين بإرتكاب هذه الجرائم وتيسير إجراءات تسليمهم بين الدول.

6. ضرورة التوعية بالمخاطر المصاحبة لإستخدام شبكة الإنترنت ، خاصةً فى الإستخدامات

التجارية وكذلك ضرورة توعية أولياء الأمور من إستخدام أبنائهم للإنترنت خشية وقوعهم ضحايا لجرائم الإستغلال الجنسى.

7. إضافة نصوص إلى قانون الإجراءات الجنائية فيما يتعلق بالمعاينة والتفتيش وضبط الأدلة ، بما يتماشى والطابع التكنولوجى للجريمة بحيث لا تتم العمليات السابقة بناء على النصوص التقليدية التى تنظمها فى قانون الإجراءات الجنائية ، بل تصاغ نصوص جديدة تبين المقصود بالتفتيش المعلوماتى مثلاً وعلى من يقع وكيف تضبط أدلة الجريمة وهل أدلة الجريمة المطلوبة فى هذه الجريمة أدلة مادية عادية أم رقمية وهكذا.

8. الإهتمام بإجراء الدراسات والبحوث العلمية التى تتناول هذه الظاهرة الإجرامية وعقد الملتقيات والمؤتمرات التى تناقشها وتبين أهم آثارها.

9. تشديد الرقابة على المكاتب التى تقدم خدمات الإنترنت والتى تعرف بإسم (مقاهى الإنترنت) ووضع نظم مراقبة تسمح بضبط أى تصرف خارج عن نطاق إستخدام الشبكة ، مع مراعاة خصوصيات المستخدم.

10. قيام الدولة بإجبار الجهات المسئولة عن تقديم خدمات الإنترنت بإستخدام نظم منع وحجب المواقع الضاره والمواقع ذات الطابع الإباحى ، والتى أثبتت الإحصائيات تضخم عدد مرتاديها.

11. الإستعانة بالخبرات الأجنبية فى مواجهة جرائم الإنترنت ، لاسيما الدول التى أحرزت تقدماً فى السيطرة على المد الإجرامى لهذه الظاهرة.

12. وضع مقررات دراسية في مناهج كليات الحقوق والشرطة تتضمن الشرح الوافى عن شبكة الإنترنت ، وماهيتها وما هى الجرائم التى ترتكب أو من الممكن إرتكابها من خلالها ، وإبراز خصائص ودوافع مرتكبى هذه الجرائم.

وختاماً أرجو أن يكون بحثى هذا قد أصاب ولو القليل من الصواب ، فإن كان فهو من عند الله وإن لم يكن فكذلك الحمد لله.

تم بحمد الله وتوفيقه

قائمـــة المراجــع

أولاً: المراجــع العربيـــة:

(أ) المؤلفــات العامـة:

1. د/ أحمد أمين بك : شرح قانون العقوبات المصرى ، القسم الخاص، بدون ناشر، 1949.
2. د/ أحمد فتحى سرور: الوسيط فى قانون العقوبات ، القسم الخاص ، الطبعة الرابعة ، دار الطباعة الحديثة ، 1991.
3. د/ إدوارد غالى الدهبى : شرح قانون العقوبات القسم الخاص ، دراسة مقارنة للقانون الليبى والقوانين العربية والأجنبية ، الطبعة الثانية ، مكتبة غريب ، 1976.
4. د/ جلال ثروت : نظم القسم الخاص فى قانون العقوبات، منشأة المعارف، 2000.
5. د/ حسنين إبراهيم صالح عبيد : جرائم الإعتداء على الأشخاص ، دارالنهضة العربية ، 1983.
6. د/ رمسيس بهنام : القسم الخاص فى قانون العقوبات،دار المعارف، الطبعة الاولى، 1958.
7. د/ عمر السعيد رمضان : شرح قانون العقوبات القسم الخاص، دار النهضة العربية ، 1986،.
8. د/ عوض محمد عوض : المبادئ العامة في قانون الإجراءات الجنائية ، دار المطبوعات الجامعية ، 1999.
9. د/ فائزة يونس الباشا : القانون الجنائى الخاص الليبى القسم الأول جرائم الإعتداء على الأشخاص ، دار النهضة العربية، بدون تاريخ.
10. د/ فوزية عبد الستار : شرح قانون العقوبات القسم الخاص ، الطبعة الثانية ، دار النهضة العربية ، 1988.
11. د/ ماجد راغب الحلو : العقود الإدارية، دار الجامعة الجديدة،2007.
12. د/ مأمون محمد سلامة : قانون الإجراءات الجنائية معلقاً عليه بالفقه وأحكام النقض ، الطبعة الثانية ، 2005 ، بدون دار نشر.
13. د/ محمد زكى أبو عامر : قانون العقوبات ، القسم الخاص ، دار الجامعة الجديدة ، 2007.

14. د/ محمود نجيب حسنى : شرح قانون العقوبات القسم الخاص، ، دار النهضة العربية ، 1978.

15. د/ محمود مصطفى : شرح قانون العقوبات القسم الخاص ، الطبعة الثامنة ، دار النهضة العربية ، 1984.

(ب) المؤلفـــات الخاصـــة:

1. د/أحمد عبد الكريم سلامة: قانون حماية البيئة ، دراسة تأصيلية في الأنظمة الوطنية والإتفاقية ، الطبعة الأولى ، منشورات جامعة الملك سعود . السعودية ، 1997.

2. أسامة أحمد المناعسة ، جلال محمد الزعبي ، صايل فاضل الهواوشة : جرائم الحاسب الآلى والإنترنت ، دراسة تحليلية مقارنة ، الطبعة الأولى ، داروائل للنشر والتوزيع ، عمان ، 2001.

3. د/ جميل عبد الباقى الصغير:

- أدلة الإثبات الجنائى والتكنولوجيا الحديثة ، دراسة مقارنة ، دار النهضة العربية ، 2002.
- الجوانب الإجرائية للجرائم المتعلقة بالإنترنت ، دار النهضة العربية ، 1998.
- الحماية الجنائية والمدنية لبطاقات الإئتمان الممغنطة ، دار النهضة العربية ، 1999
- القانون الجنائى والتكنولوجيا الحديثة ، الكتاب الأول ، الجرائم الناشئة عن إستخدام الحاسب الآلى ، دار النهضة العربية ، 1992.

4. د/ حسنين إبراهيم صالح عبيد: القضاء الجنائى الدولى ، (تاريخه . تطبيقاته . مشروعاته) ، دار النهضة العربية ،1977.

5. حسن حسن منصور: جرائم الإعتداء على الأخلاق ، دار المطبوعات الجامعية ، 1985.

6. مهندس /حسن طاهر داوود: جرائم نظم المعلومات، جامعة نايف العربية للعلوم الامنية،الطبعة الاولى ،الرياض 1420هـ.

7. د/ خالد بن سليمان الغثير ، د/ محمد بن عبد الله القحطانى: أمن المعلومات بلغة ميسرة ، مركز التميز لأمن المعلومات جامعة الملك سعود ، الطبعة الأولى ، 2009 .

8. د/ ذياب البداينة: جرائم الحاسب والإنترنت ، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها ، أكاديمية نايف للعلوم الأمنية ، الرياض ، 1420هـ.

9. المهندس / رأفت رضوان: إتجاهات مجتمع الأعمال العربى نحو التجارة الإليكترونية ، بدون دار نشر ، 1999.

10. د/ سعيد عبد اللطيف حسن: إثبات جرائم الكمبيوتر والمرتكبة عبر الإنترنت ، دار النهضة العربية ، 1999.

11. د/ سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية دار النهضة العربية ،2007.

12. د/ طارق إبراهيم الدسوقى عطية: د الأمن المعلوماتى (النظام القانونى للحماية المعلوماتية) ، دار الجامعة الجديدة ، 2009.

13. د/ عبد الفتاح بيومى حجازى :

- الجرائم المستحدثة فى نطاق التكنولوجيا الحديثة، منشاة المعارف ،الطبعة الأولى، 2009.
- الحكومة الإليكترونية ونظامها القانونى، المجلد الأول، النظام القانونى للحكومة الاليكترونية، دار الفكر الجامعى ،2004.
- الدليل الجنائى والتزوير فى جرائم الكمبيوتر والإنترنت ، دار الكتب القانونية ، 2002.
- نحو صياغة نظرية عامة فى علم الجريمة والمجرم المعلوماتى، ، بدون دار نشر، الطبعة الأولى، 2009.
- النظام القانونى لحماية التجارة الإليكترونية ، المجلد الأول :نظام التجارة الإليكترونية وحمايتها مدنياً ، الطبعة الأولى، دار الفكر الجامعى ، 2002.

14. د/ عبد الرحمن عبد العزيز السبيعى : حرب المعلومات، مرامر للطباعة الإليكترونية، بدون تاريخ.

15. د/ عفيفي كامل عفيفى : جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ، بدون ناشرأو تاريخ.

16. د/ على بن عبد الله عسيرى : الآثار الأمنية لإستخدام الشباب للإنترنت، جامعة نايف العربية للعلوم الامنية ، الطبعة الأولى الرياض،1425هـ.

17. د/ عمر فاروق الحسينى: المشكلات الهامة المتصلة بالحاسب الآلى وأبعادها الدولية ، دراسة تحليلية ونقدية لنصوص التشريع المصرى مقارناً بالتشريع الفرنسى ، ط2، دار النهضة العربية، 1995.

18. د/ فائزة يونس الباشا: الجريمة المنظمة في ظل الإتفاقيات الدولية والقوانين الوطنية ، دار النهضة العربية ، الطبعة الأولى ، 2001.

19. محمد عبيد الكعبى: الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت ، دراسة مقارنة ، دار النهضة العربية، بدون تاريخ.

20. د/ محمد عبد الله أبو بكر سلامة : موسوعة جرائم المعلوماتية (جرائم الكمبيوتر والإنترنت) ، منشأة المعارف ، 2006.

21. د/ محمد أمين الشوابكة : جرائم الحاسوب والإنترنت (الجريمة المعلوماتية) ، دار الثقافة للنشر والتوزيع ، عمان ، 2007.

22. د/ محمد حسين منصور: المسئولية الإليكترونية ، دار الجامعة الجديدة ، 2003.

23. اللواء د/ محمد الأمين البشرى: التحقيق فى الجرائم المستحدثة ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، الطبعة الأولى ، 1425هـ .

24. اللواء د/ محمد فتحى عيد : الإنترنت ودوره فى إنتشار المخدرات ، أكاديمية نايف العربية للعلوم الأمنية ، الرياض ، 1424هـ.

25. د/ محمد فهمى : الموسوعة الشاملة لمصطلحات الحاسب الآلى الإليكترونى ، مطابع المكتب المصرى الحديث ، 1991 .

26. د/ محمود أحمد عنابة : جرائم الحاسوب وأبعادها الدولية ، دار الثقافة للنشر والتوزيع ، عمان ، 2005.

27. د/ مدحت عبد الحليم رمضان : الحماية الجنائية للتجارة الإليكترونية ، دراسة مقارنة ، دارالنهضة العربية، بدون تاريخ.

28. د/ مصطفى أحمد عبد الجواد حجازى : الحياة الخاصة ومسئولية الصحفى ، دار الفكر العربى ، 2000 / 2001.

29. د/ منصور السعيد ساطور: جريمتى القذف والسب بحث مقارن فى القانون الجنائى الوضعى والفقه الجنائى الإسلامى ، بدون دار نشر ، 1980.

30. نبيلة هبة هروال: الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الإستدلالات، دراسة مقارنة، دار الفكر الجامعى، الاسكندرية،2007.

31. د/هدى قشقوش : جرائم الحاسب الإليكتروني في التشريع المقارن، الطبعة الأولى ، دار النهضة العربية، القاهرة، 1992.

32. د/هشام محمد فريد رستم : الجوانب الإجرائية للجرائم المعلوماتية (دراسة مقارنة) ، مكتبة الآلات الحديثة ، أسيوط ، 1994.

33. د/ هلالى عبد اللاه أحمد :

- إلتزام الشاهد بالإعلام فى الجريمة المعلوماتية ، دراسة مقارنة ، دار النهضة العربية ، 2006.
- تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى ، دراسة مقارنة ، دار النهضة العربية ، 2006.

34. د/ يحيى مصطفى حلمى وآخرون : أساسيات الحاسبات الاليكترونية، مكتبة عين شمس ،القاهرة،1995.

(ج) الرسائل العلمية:

1. د/ إبراهيم الغماز: الشهادة كدليل إثبات فى المواد الجنائية ، رسالة دكتوراه ، كلية الحقوق ، جامعة القاهرة ، 1980.

2. د/ حسين بن سعيد الغافرى : السياسة الجنائية فى مواجهة جرائم الإنترنت (دراسة مقارنة) ، رسالة دكتوراه ، كلية الحقوق ، جامعة عين شمس.

3. سالم محمد سليمان الأوجلى: أحكام المسئولية الجنائية عن الجرائم الدولية فى التشريعات الوطنية ، دراسة مقارنة (رسالة دكتوراه) كلية الحقوق ، جامعة عين شمس ، 1997 .

4. عبد الرحمن محمد بحر: معوقات التحقيق في جرائم الإنترنت : دراسة مسحية على ضباط الشرطة في دولة البحرين ، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية. (1420هـ).

5. د/عمر محمد أبوبكر بن يونس: الجرائم الناشئة عن إستخدام الإنترنت ، رسالة دكتوراه ، كلية الحقوق ، جامعة عين شمس ، 2004 .

(د) البحوث والدراسات:

1. د/ أبو المعالي محمد عيسى: بحث بعنوان: الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية ،مقدم إلى المؤتمر المغاربي الأول حول: (المعلوماتية والقانون) ، المنعقد في الفترة من 28.29 أكتوبر 2009 ، أكاديمية الدراسات العليا ، طرابلس ، ليبيا.

2. أ/أولريش سيبر: جرائم الحاسب الآلي والجرائم الأخرى المرتبطة بالتقنيات الحديثة لوسائل الإتصال، ترجمة الدكتور سامي الشوا، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، 25–28، أكتوبر 1993.

3. جان فرانسوا هنروت: أهمية التعاون الدولى والتجربة البلجيكية فى تبادل المعلومات بين عناصر الشرطة والتعاون القضائى ، بحث مقدم إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر ، ضمن برنامج تعزيز حكم القانون فى بعض الدول العربية " مشروع تحديث النيابات العامة" ، المملكة المغربية ، فى الفترة من 19 . 20 يونيو 2007.

4. أ/ رحاب عميش: الجريمة المعلوماتية ، بحث مقدم إلى المؤتمر المغاربي الأول حول (المعلوماتية والقانون) ، المنعقد في الفترة من 28 . 29 أكتوبر 2009 ، أكاديمية الدراسات العليا ، طرابلس ، ليبيا.

5. الرائد الدكتور/عبد الله حسين علي محمود: إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات ، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، أكاديمية شرطة دبي ، مركز البحوث والدراسات ، 26 . 28 /4/ 2003 ، دبي – الإمارات العربية المتحدة .

6. الرائد/على حسنى عباس: مخاطر بطاقات الدفع الإليكترونى عبر شبكة الإنترنت (المشاكل والحلول) ، ورقة عمل مقدمة إلى ندوة (الصور المستحدثة لجرائم بطاقات الدفع الإليكترونى) مركز بحوث الشرطة بأكاديمية الشرطة ، القاهرة ، بتاريخ 1998/12/14.

7. عماد على الخليل: التكييف القانونى لإساءة إستخدام أرقام البطاقات الإئتمانية عبر الإنترنت ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد بكلية الشريعة والقانون بجامعة الإمارات العربية المتحدة فى الفترة من 1 : 2000/5/3.

8. د/ محمد المرسى زهرة: الدليل الكتابى وحجية مخرجات الكمبيوترفى الإثبات فى المواد المدنية والتجارية ، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت ، كلية الشريعة والقانون ، جامعة الإمارات العربية المتحدة ، الفترة من 1 : 3 /2000/5.

9. د/ محمد عبد الرحمن سلطان العلماء: جرائم الإنترنت والإحتساب عليها ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت ، كلية الشريعة والقانون ، جامعة الإمارات العربية المتحدة ، 1 : 3 /5 /2000.

10. د/محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية ، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، اكادمية شرطة دبي ، مركز البحوث والدراسات ، 26.28/4/ 2003 ، دبي ، الإمارات العربية المتحدة.

11. اللواء دكتور/ محمد الأمين البشرى: بحث بعنوان تأهيل المحققين فى جرائم الحاسب الآلى وشبكات الإنترنت ، بحث مقدم فى إطار حلقة علمية عقدت بالقاهرة تحت عنوان (الإنترنت والإرهاب) فى الفترة من 15.19/11/2008 ، جامعة نايف العربية بالتعاون مع جامعة عين شمس.

12. د/ موسى مسعود أرحومة:

- الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية ، بحث مقدم إلى المؤتمر المغاربي الأول حول (المعلوماتية والقانون) ، المنعقد في الفترة من 28.29 أكتوبر 2009.
- السياسة الجنائية في مواجهة جرائم الإنترنت ، بحث مقدم إلى مؤتمر التنمية البشرية في عالمٍ متغير، جامعة الطفيلة (الأردن) فى الفترة من 10-12/7/2007.

13. د/ نضال الشاعر: حماية الأطفال من سوء إستخدام الإنترنت وجرائم المعلوماتية ، مداخلة ضمن مؤتمر تشريعات الطفولة والعائلة في لبنان في إطار القواعد الدستورية والحقوقية ، 25/6/2006.

(هـ) المجلات والصحف:

1. د/ محمد خليفة العمرى: واقع إستخدام الإنترنت لدى أعضاء هيئة التدريس وطلبة جامعة العلوم والتكنولوجيا الأردنية، مجلة إتحاد الجامعات العربية،العدد 40،ربيع الثانى 1423هـ.

2. محمد عبد اللطيف عبد العال: حول مفهوم الشرف والإعتبار فى جرائم القذف والسب، مجلة الأمن والقانون، العدد الثانى، أكاديمية شرطة دبى بالإمارات العربية المتحدة ، يوليو 2003م.

3. جريدة الأهرام، العدد44692 ، بتاريخ17-4-2009 .

ثانياً: المراجــع الأجنبيـــة:

Second: Foreign References :

(a) Books :

1. Eric J. Sinrod، and William P Reilly، “Cyber-Crimes: A practical approach to the Application of Federal Computer Crimes Laws،16 Santa Clara computer and High Tech L.J 177، (2000)
2. Mohrenschloager (Manfred): Computer crimes and other crimes against information technology in Germany "R.I.D.P 1993.
3. Orin S. Kerr , Digital evidence and the new criminal procedure, 2005, available at, http://www.jstor.org/pss/4099310
4. Tom forester, Essential proplems to Hi-Tech Society , First MIT Pres edition, Cambridge, Massachusetts, 1989
5. Walter Gary Sharp، Redefining National Security in Today’s World of information technology and Emergent Threats، 9 Doke J Comp and Int’l (1999)

(b) Research and Studies :

1. Glenn Wahlert, Crime In Cyberspace: Trends In Computer Crime In Australia, Paper Presented at the conference: Internet Crime, held in Melbourne, 16-17 February 1998, by the Australian Institute of Criminology,p4.
2. Dr.Peter Grabosky , Crime And Technology In The Global Village, Paper Presented at:The Conference: Internet Crime, held in Melbourne, 16-17 February 1998, by the Australian Institute of Criminology.
3. Raphael F. Perl , Terrorist Use of the Internet Threat, Issues, and Options for International Co-operation , Second International Forum on Information Security, Garmisch-Partenkirchen, 7-10 April 2008.
4. Russell G. Smith , Paying The Price On The Internet, Funds Transfer Crime In Cyberspace, Paper presented at the conference: Internet Crime, held in Melbourne, 16-17 February 1998, by the Australian Institute of Criminology.

ثالثاً: القوانين:

1. قانون العقوبات المصرى رقم 58 لسنة 1937 والمعدل بموجب القانون رقم 95 لسنة 2003 والقانون رقم 147 لسنة 2006.
2. قانون العقوبات الليبى الصادر سنة 1953 وفقاً لأحدث تعديلاته.
3. القانون رقم 52 لسنة 1974م فى ليبيا بشأن إقامة حد القذف.
4. القانون رقم "20 لسنة1991م" بشأن تعزيز الحرية فى ليبيا.
5. قانون الطفل فى مصر المعدل بالقانون رقم 126 لسنة 2008.
6. قانون التوقيع الإليكترونى رقم 15 لسنة 2004 فى مصر
7. القانون رقم 82 لسنة 2002 بشأن حقوق الملكية الفكرية فى مصر.
8. القانون رقم 80 لسنة 2002 والمعدل بالقانون رقم 78 لسنة 2003. بشأن غسيل الأموال فى مصر.
9. القانون رقم (2) لسنة1373و.ر2005م بشأن مكافحة غسيل الأموال فى ليبيا.
10. قانون تنظيم الصحافة رقم 96 لسنة 1996 فى مصر.
11. دستور جمهورية مصر العربية 1971.
12. نظام مكافحة الجرائم المعلوماتية السعودى الصادر بقرار مجلس الوزراء رقم (79) بتاريخ 1428/3/7هـ .

رابعــاً: شبكــة الإنــترنت:

(1) البحوث والمقالات المنشورة على شبكة الإنترنت:

(أ) باللغـة العربيـة:

1. إنعام محسن غدير ، سارة مشير عبد الهادي: مقال بعنوان ، غسيل الأموال .. مراحله ، طرقه والآثار الناجمة عنه ، بالموقع الإليكترونى:

http://www.free-pens.org/index.php?show=news&action=article&id=141

2. د/ حسين بن سعيد الغافرى / بحث بعنوان جهود السلطنة فى مواجهة جرائم الإنترنت ، البحث منشور بالموقع الإليكترونى:

http://www.eastlaws.com/Others/ViewMorafaat.aspx?ID=2

3. د/ حسين بن سعيد الغافري : مقال بعنوان الإباحية على شبكة الإنترنت ، بالموقع الإليكترونى: http://www.omanlegal.net/vb/showthread.php?t=441

4. د/ حسين بن سعيد الغافرى : بحث بعنوان الجرائم الواقعة على التجارة الإليكترونية ، بالموقع الإليكترونى :

http://www.eastlaws.com/Others/ViewMorafaat.aspx?ID=4

5. د/ حسين بن سعيد الغافرى : بحث بعنوان التحقيق وجمع الأدلة فى الجرائم المتعلقة بشبكة الإنترنت ، البحث منشور بالموقع الإليكترونى:

http://www.eastlaws.com/Others/ViewMorafaat.aspx?ID=33

6. د/ خالد ممدوح إبراهيم : حجية البريد الإليكتروني في الإثبات،بحث منشور بالموقع الإليكترونى:

http://www.tashreaat.com/view_studies2.asp?id=658&std_id=9

7. د/ صالح أحمد البربري : بحث بعنوان ، دور الشرطة في مكافحة جرائم الإنترنت في إطار الإتفاقية الأوروبية ، منشور بالموقع الإليكترونى:

http://lawjo.net/vb/showthread.php?p=6024

8. د/ صبرى الحاج المبارك : مقال بعنوان المعلومات ودورها فى التنمية ، بالموقع الإليكترونى: http://informatics.gov.sa/details.php?id=295

9. د /عبد الله بن عبد العزيز الموسى : مقال بعنوان إستخدام خدمات الانترنت بفاعلية فى التعليم، منشور بالموقع الإليكتروني:

www.riyadhedu.gov.sa/alan/fntok/12.htm

10. عبد المنعم حلاق : جريدة الفداء السورية ، مقال بعنوان النظام العام والآداب العامة ، بالموقع الإليكترونى:

http://fedaa.alwehda.gov.sy/_archive.asp?FileName=4895092892009120618223

11. عثمان سعيد المحيشي : ورقة عمل مقدمه إلى المنظمة العربية للتنمية الإدارية، المؤتمر الدولي الأول لقانون الإنترنت21-25 اغسطس2005 ، بالموقع الإليكترونى:

http://www.minshawi.com/other/muhashy.htm

12. عماد مهدى : بحث إجتماعى بعنوان توظيف التقنية الحديثة لمعالجة ومكافحة الجرائم الأخلاقية ، بالموقع الإليكترونى: http://emad-7272.maktoobblog.com

13. فادي سالم : مقال بعنوان موقعك في ويب.. في مهب الاختراق ، صحيفة الحوار المتمدن الإليكترونية ، العدد رقم: 15 بتاريخ 12/23 /2001 ، بالموقع الإليكترونى:

http://www.ahewar.org/debat/show.art.asp?aid=550

14. د/ فؤاد جمال: جرائم الحاسبات والإنترنت ،بحث منشور بالموقع:

http://www.tashreaat.com/view_studies2.asp?id=592&std_id=90

15. د/ قاسم النعيمى : التجارة الإليكترونية بين الواقع والحقيقة ، بحث منشور بالموقع الإليكترونى: jps-dir.com/Forum/uploads/1364/qaseem.doc

16. ليال كيوان: تحقيق بعنوان الاستغلال الجنسي للأطفال عبر الانترنت أو "بورنو الأطفال"، جريدة النهار اللبنانية ، بتاريخ 17 /5 /2009 ، بالموقع الإليكترونى:

http://www.annahar.com.

17. د/ محمد ياسر أبو الفتوح : مقال بعنوان خصائص وتصنيفات الجريمة المعلوماتية ، بالموقع الإليكترونى:

http://www.shaimaaatalla.com/vb/showthread.php?t=3951

18. د/ محمد عبد الله المنشاوى : بحث بعنوان جرائم الانترنت من منظور شرعي وقانوني ، بالموقع الإليكترونى:

http://www.minshawi.com/old/internetcrim-in%20the%20law.htm

19. محمد محمد صالح الألفى : بحث بعنوان بعض أنماط الجرائم الأخلاقية عبر الإنترنت فى المجتمع العربى بالموقع الإليكترونى:

http://www.eastlaws.com/Others/ViewMorafaat.aspx?ID=119

20. د/ محمد إبراهيم محمود الشافعى : مقال بعنوان النقود الإلكترونية(ماهيتها، مخاطرها وتنظيمها القانوني) بالموقع الإليكترونى:

http://www.manqol.com/topic/?t=7651

21. د/ مشعل بن عبد الله القدهى : مقال بعنوان المواقع الإباحية على شبكة الإنترنت ، بالموقع الإليكترونى: http:// www.minshawi.com/gadhi.htm

22. د/ معتز محيي عبد الحميد : مقال بعنوان الإستغلال الجنسي للأطفال ، بالموقع الخاص بجريدة الصباح العراقية:

http://www.alsabaah.com/paper.php?source=akbar&mlf=interpage&sid=17059

23. وجدي عبد الفتاح سواحل : مقال بعنوان فيروسات الكمبيوتر الكابوس الدائم، منشور على بالموقع الإليكتروني:

www.islamonline.net/serviet/satellite?c=articleA.

24. القاضى وليد عالكوم : بحث بعنوان التحقيق فى جرائم الحاسوب ، البحث منشور بالموقع الإليكترونى: http://www.4shared.com/file/WLlIhQTH/__html

25. المحامى/ يونس عرب : بحث بعنوان جرائم الكمبيوتر والإنترنت المعنى والخصائص والصور وإستراتيجية المواجهة القانونية، بحث منشور على الانترنت، بالموقع الإليكترونى: http://doc.abhatoo.net.ma/spip.php?article1200

26. المحامى/ يونس عرب : مقال بعنوان ، جرائم غسيل الأموال دراسة في ماهية ومخاطر جرائم غسيل الأموال، والإتجاهات الدولية لمكافحتها ، بالموقع الإليكترونى:

www.foca.net/AR/Money_Laundry_Crimes.doc

27. مقال بعنوان السعودية تطبق أول حكم قضائي فى جرائم الإنترنت:

http://islamtoday.net/bohooth/artshow-50-105674.htm

28. تحقيق بعنوان مواجهة حاسمة من الشرطة لجرائم بطاقات الائتمان الإلكترونية ، جريدة الأهرام ، بتاريخ 2002/5/18، السنة 126 ، العدد 42166 ، بالموقع الإليكترونى:

http://www.ahram.org.eg/Archive/2002/5/18/ECON5.HTM

29. مقال بعنوان جرائم الإنترنت التي تستهدف القاصرين ، بالموقع الإليكترونى:

http://www.jeunessearabe.info/article.php3?id_article=580

30. مقال بعنوان جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت ، بالموقع الإليكتروني: www.arblaws.com.

31. مقال بعنوان غسيل الأموال تعريفها وخصائصها ، بالموقع الاليكترونى:

http://www.titanic-arwad.com/vb/showthread.php?t=13866

32. مقال بعنوان ، تشفير البيانات فى إنترنت ، بالموقع الإليكترونى:

http://www.arabteam2000-forum.com/index.php?showtopic=5441

(ب) باللغة الإنجليزية:

(b) Articles in English:

1. An article entitled : Abrief history of the internet. available at: http://www.walthowe.com/navnet/history.html

2. Daniel Larkin: an article entitled, fight cybercrime. available at: http://www.america.gov/st/democracy-arabic/2008/May/20081117124 454 snmassabla0. 2601086.htm.
3. Daniel A Morris , an article entitled, tracking a Computer Hacker ، USA Bulletin ، available at http://www.justice.gov/ criminal/cybercrime/ usamay2001_2.htm
4. Jason Bennetto : an article entitled, Police launch a cyber squad to combat growth of Internet crime. available at: http://www.independent. co .uk/news/business/analysis-and-features/ police-launch-a-cyber-squad-to-combat-growth-of-internet-crime-743235.html.
5. Dr. Phil Williams : An article entitled , Organized crime And crimes of the Internet. available at:http://usinfo.state.gov/journals/itgic/ 0801/ijga/comntry3.htm

(2) مواقع الإنترنت الأخرى:

1. www.goa.gov
2. www.oecd.org
3. http://www.moj.gov.om/ موقع وزارة العدل بسلطنة عمان
4. http://reda79.jeeran.com/laweg/archive/2008/5/571259.html
5. http://www.djelfa.info/vb/showthread.php?t=204052
6. http://www.al-jazirah.com.sa/digimag/20062004/wr25.htm
7. http://www.arab-elaw.com/show_similar.aspx?id=93
8. http://arabhardware.net/forum/archive/index.php/t-42072.html
9. http://www.prameg.com/vb/t66778.html
10. http://download.paramegsoft.com/news-52
11. http://jmuslim.naseej.com/Detail.asp?InNewsItemID=273160
12. ttp://www.nasbcom.net/vb/showthread.php?t=7208h
13. http://lattakia.org/ShowArticle.aspx?ID=212&AspxAutoDetectCookieSupport=1
14. http://forums.mixolgy.net/t126490.html
15. www.albayan.co.ae/albayan/mnw/15.htm
www.gulfpark.com/showarticale.php?cat=news&article-id=252
16. http://www.al-jazirah.com.sa/digimag/20062004/wr25.htm

17. www.khayma.com/tanweer/textes/hacar.htm
18. http://www.fursansouria.org/acg/domain_name_definition.html

البوابة العربية للكمبيوترعلى الإنترنت

19. http://www.europol.europa.eu موقع الشرطة الأوروبية على الإنترنت
20. http://www.moiegypt.gov.eg/Arabic/Departments+Sites/Media+and +public+Relation/Conferences/mo07042009.htm
21. Tunis Agenda For The Information Society available at :http://www .itu.int/wsis/docs2/tunis/off/6rev1.html أجندة تونس
22. http://www.f-law.net/law/showthread.php?10802
23. http://www.f-law.net/law/showthread.php?10801
24. http://www.egypty.com/accidents-details.aspx?accidents=3030
25. http://citizen-service.moiegypt.gov.eg/crimes_web/main.htm

موقع وزارة الداخلية المصرية

26. www.fbi.gov موقع مكتب التحقيقات الفيدرالى على الإنترنت
27. http://www.interpol.int موقع الإنتربول على الإنترنت
28. http://www.delsyr.ec.europa.eu/ab/europe_in_12_lessons/10.html
29. www.interpol.int/Public/ICPO/LegalMaterials/FactSheets/FS11ar. pdf نشرة الإنتربول الإعلامية
30. http://www.cybersecuritycooperation.org/moredocuments/International%20Agreements/55-63%20French.pdf

القرار رقم 55/63 للجمعية العامة للأمم المتحدة الذى تم تبنيه بتاريخ 4 ديسمبر 2000

31. http://shkoon.coolfreepage.com/amn/pages/amn-jra.htm
32. http://www.m3rof.com/vb/t29170.html
33. www.moheet.com/ show_files.aspx?fid=44439
34. http://www.bcblebanon.com/arabic/court_cases/internet_banks_fraud.htm#_Toc100725665
35. http://www.itep.ae/arabic/EducationalCenter/Articles/Encryption_01.asp

الفهـرس

رقم الصفحة	المـوضــــوع

الموضوع	رقم الصفحة

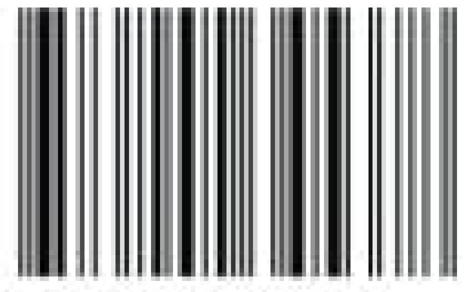
الحماية الجنائية من جرائم الإنترنت

لا يخفى الدور البارز لشبكة الانترنت في تقريب و اختصار المسافات..فلهذه التكنولوجيا ميزة كبرى ليس بمجال الاتصالات فحسب.. وانما بكافة المجالات العلميه والاقتصاديه والحكوميه..الا انها بذات الوقت قد افرزت نوعا مستحدثا من الجرائم الاليكترونيه او التقنيه التي تختلف بشكل جذري عما يناظرها من الجرائم التقليديه.. وقد حاول هذا البحث دراسة البعض من هذه الجرائم مع استقصاء طرق التأمين والحماية الممكنه بمواجهة مجرمي شبكة الانترنت... من حيث مدى قدرة كلا من القوانين العقابيه العاديه على مجاراة تلك الظاهره... والقوانين المعلوماتيه المستحدثه خصيصا في هذا الشأن.. اضافة لعرض الحلول التقنيه والفنيه التي قد تساهم في التقليل من هذه الجريمه..



نادر عبد الكريم الغزواني... ليبي الجنسيه...حاصل على ليسانس قانون 2004 من جامعة عمر المختار...ومتحصل على الماجستير في القانون العام 2014 من جامعة الإسكندريه..يعمل بوزارة العدل الليبيه... وأستاذ متعاون بكلية القانون بجامعة عمر المختار.





978-620-2-34537-8